FIG.1

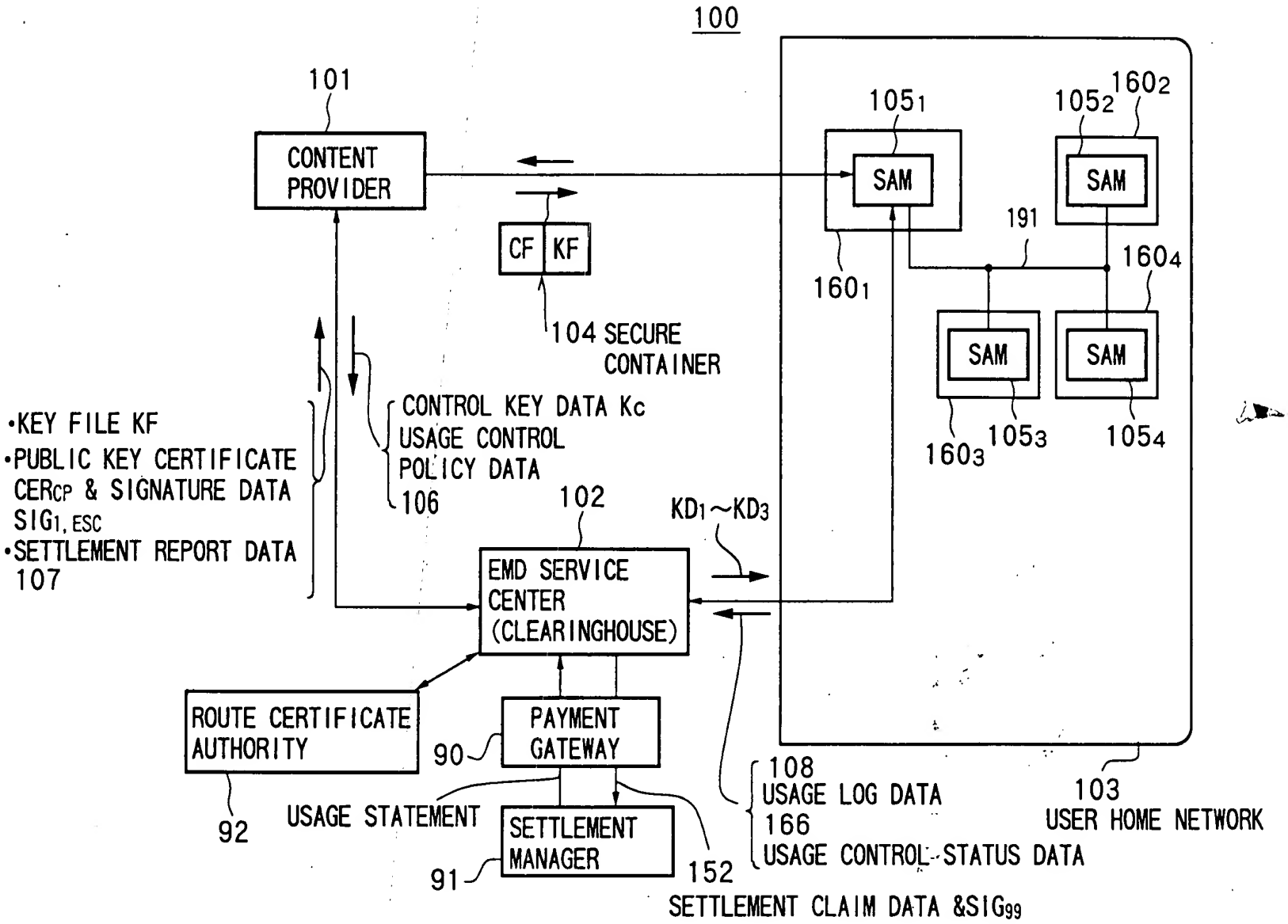


FIG.2

CONCEPT OF SECURE CONTAINER OF PRESENT INVENTION

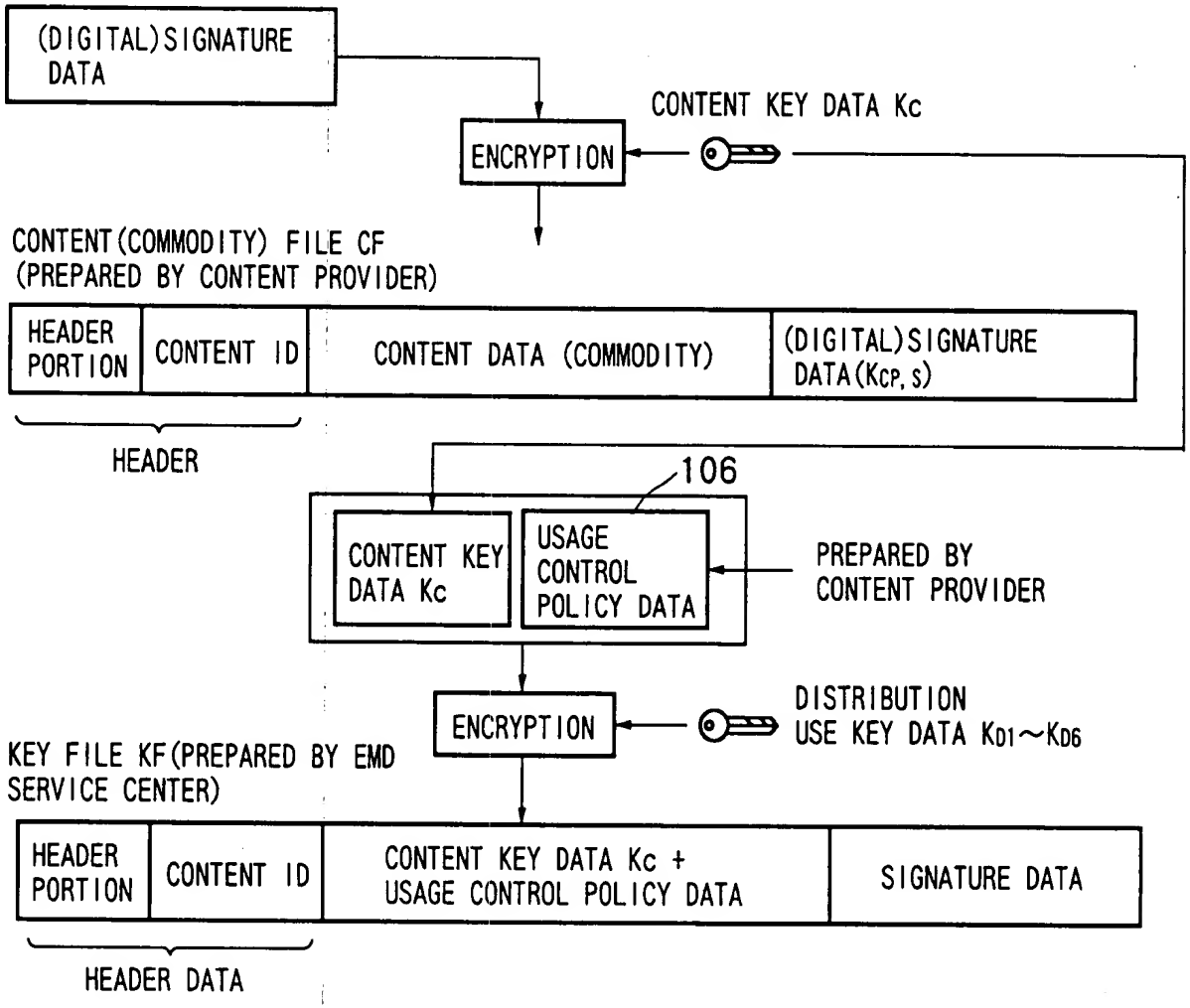


FIG.3

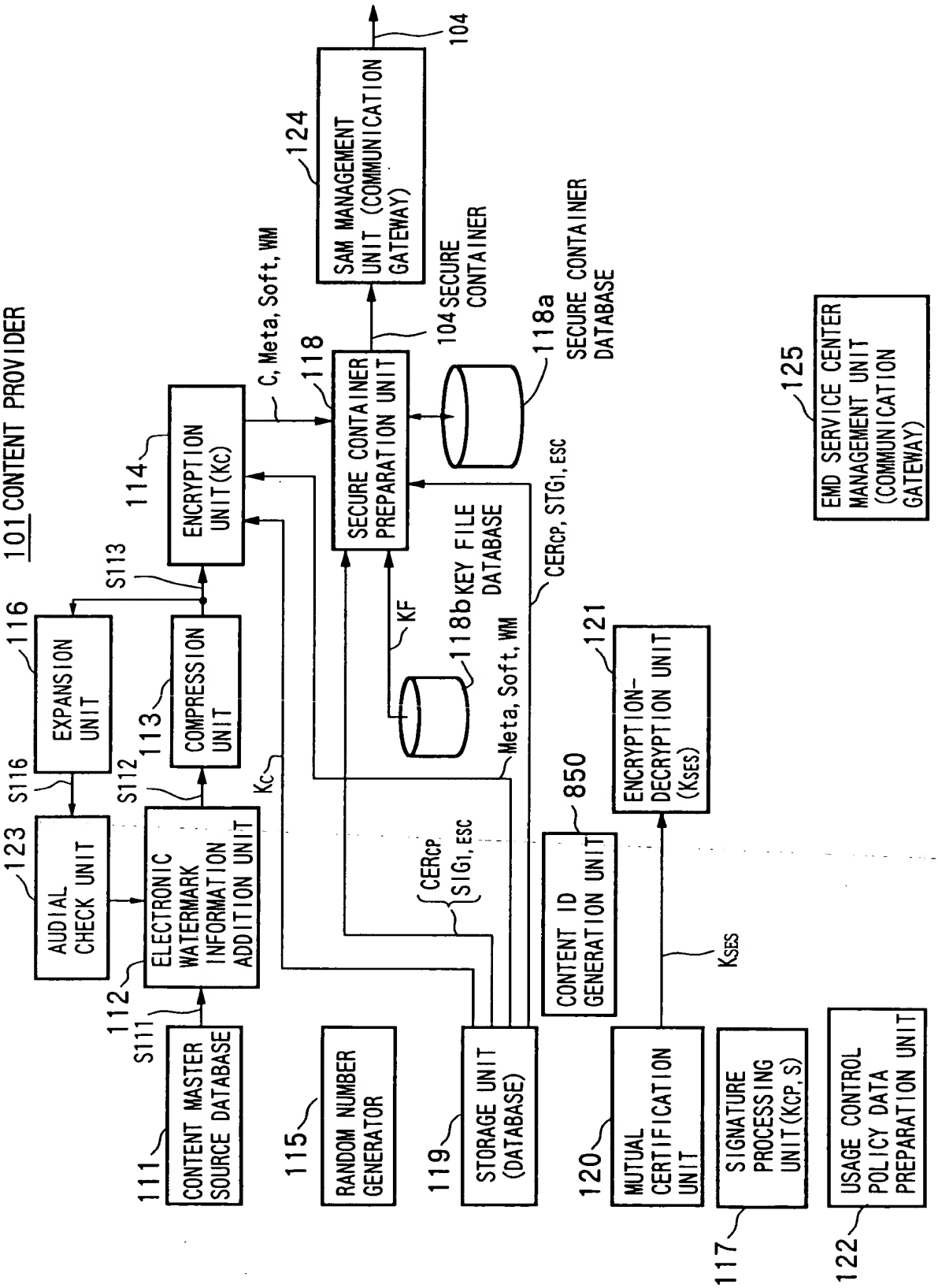

101 CONTENT PROVIDER
111 CONTENT MASTER SOURCE DATABASE
112 ELECTRONIC WATERMARK INFORMATION ADDITION UNIT
113 COMPRESSION UNIT
114 ENCRYPTION UNIT(Kc)
115 RANDOM NUMBER GENERATOR
116 EXPANSION UNIT
117 SIGNATURE PROCESSING UNIT(KCP, S)
118 SECURE CONTAINER PREPARATION UNIT
118a SECURE CONTAINER DATABASE
118b KEY FILE DATABASE
119 STORAGE UNIT (DATABASE)
120 MUTUAL CERTIFICATION UNIT
121 ENCRYPTION-DECRYPTION UNIT (KSES)
122 USAGE CONTROL POLICY DATA PREPARATION UNIT
123 AUDIAL CHECK UNIT
124 SAM MANAGEMENT UNIT (COMMUNICATION GATEWAY)
125 EMD SERVICE CENTER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
104 SECURE CONTAINER
850 CONTENT ID GENERATION UNIT
S111
S112
S113
S116
C, Meta, Soft, WM
Kc
KF
CERCP, STG1, ESC
Meta, Soft, WM
CERCP
SIG1, ESC
KSES

FIG.4

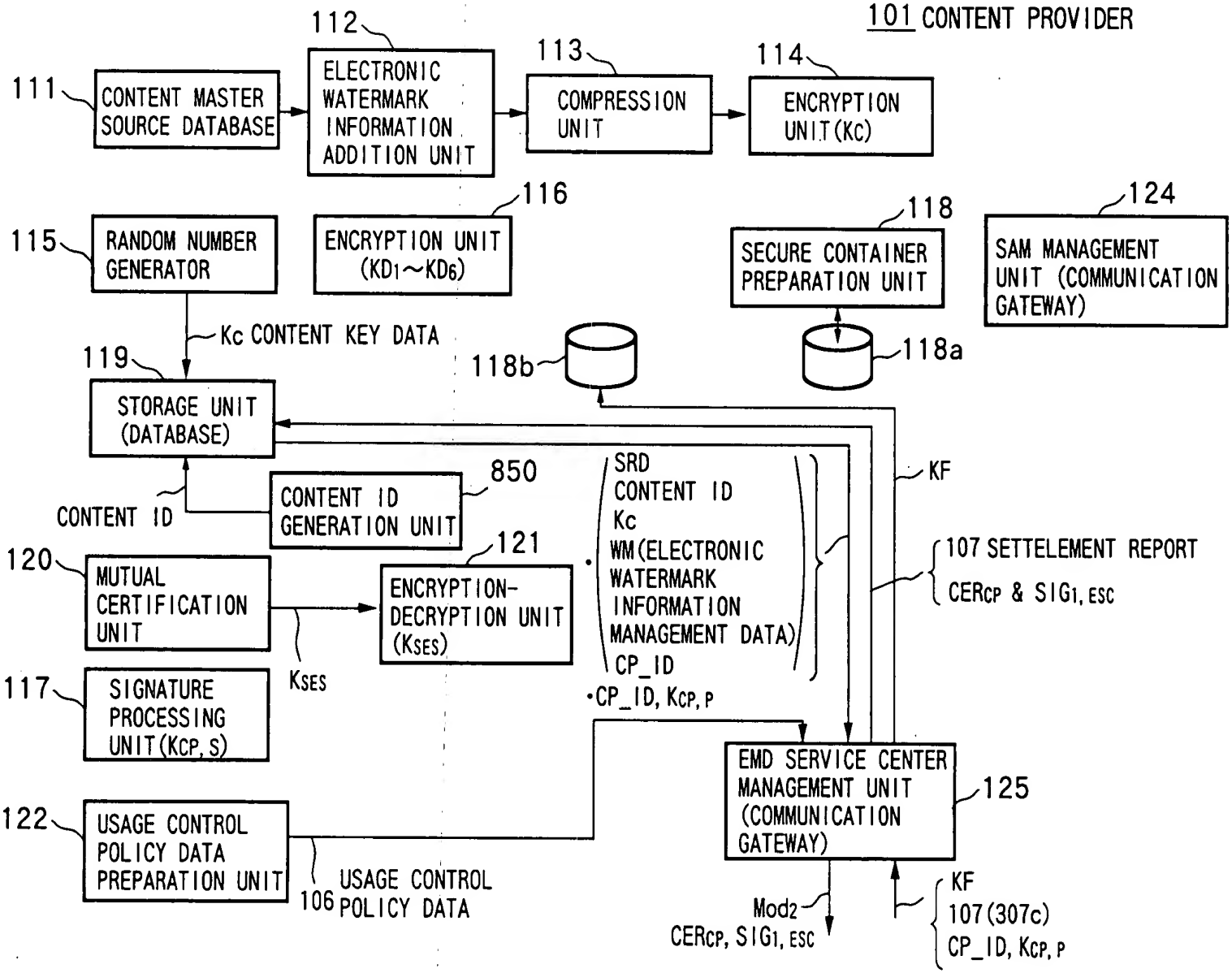


FIG.5A

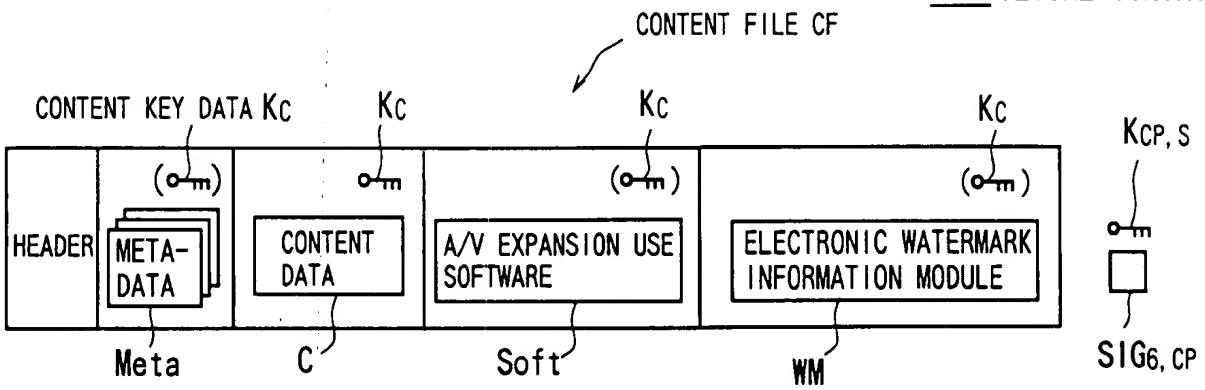


FIG.5B

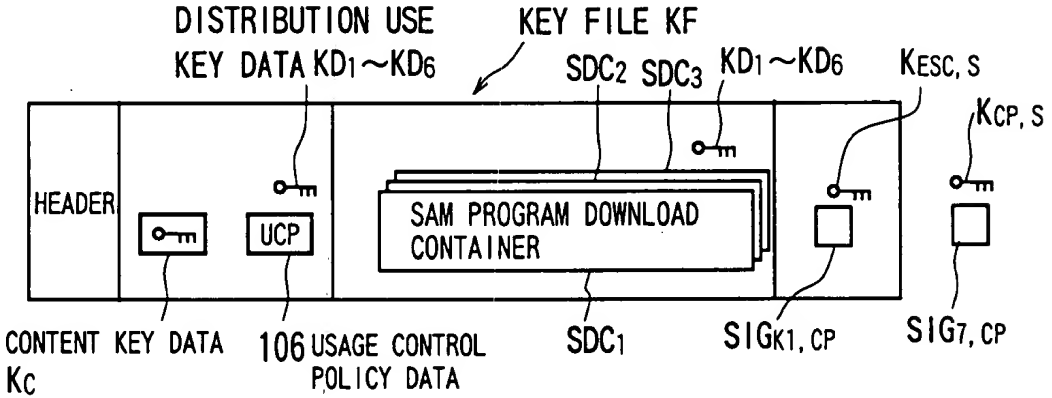


FIG.5C

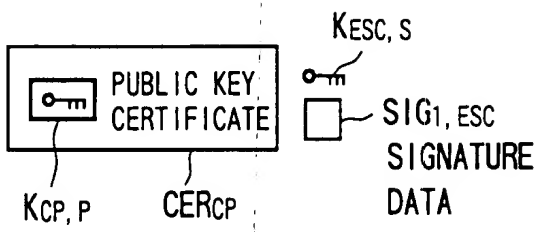


FIG.6

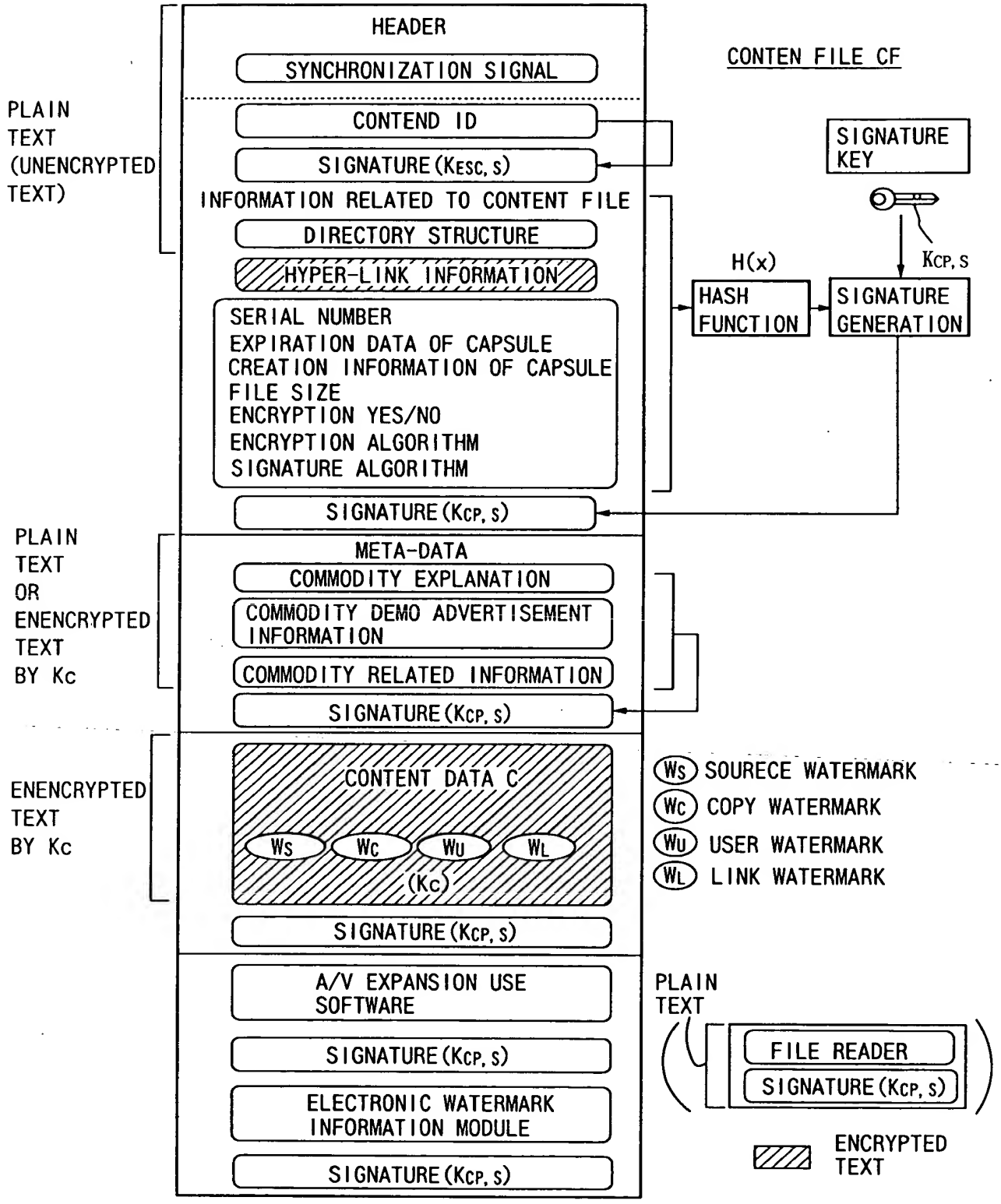

HEADER
SYNCHRONIZATION SIGNAL
CONTEND ID
SIGNATURE (KESC, S)
INFORMATION RELATED TO CONTENT FILE
DIRECTORY STRUCTURE
HYPER-LINK INFORMATION
SERIAL NUMBER
EXPIRATION DATA OF CAPSULE
CREATION INFORMATION OF CAPSULE
FILE SIZE
ENCRYPTION YES/NO
ENCRYPTION ALGORITHM
SIGNATURE ALGORITHM
SIGNATURE (KCP, S)
META-DATA
COMMODITY EXPLANATION
COMMODITY DEMO ADVERTISEMENT INFORMATION
COMMODITY RELATED INFORMATION
SIGNATURE (KCP, S)
CONTENT DATA C
WS
WC
WU
WL
(KC)
SIGNATURE (KCP, S)
A/V EXPANSION USE SOFTWARE
SIGNATURE (KCP, S)
ELECTRONIC WATERMARK INFORMATION MODULE
SIGNATURE (KCP, S)
PLAIN TEXT (UNENCRYPTED TEXT)
PLAIN TEXT OR ENENCRYPTED TEXT BY Kc
ENENCRYPTED TEXT BY Kc
CONTEN FILE CF
SIGNATURE KEY
KCP, S
H(x)
HASH FUNCTION
SIGNATURE GENERATION
WS SOURECE WATERMARK
WC COPY WATERMARK
WU USER WATERMARK
WL LINK WATERMARK
PLAIN TEXT
FILE READER
SIGNATURE (KCP, S)
ENCRYPTED TEXT

FIG.7

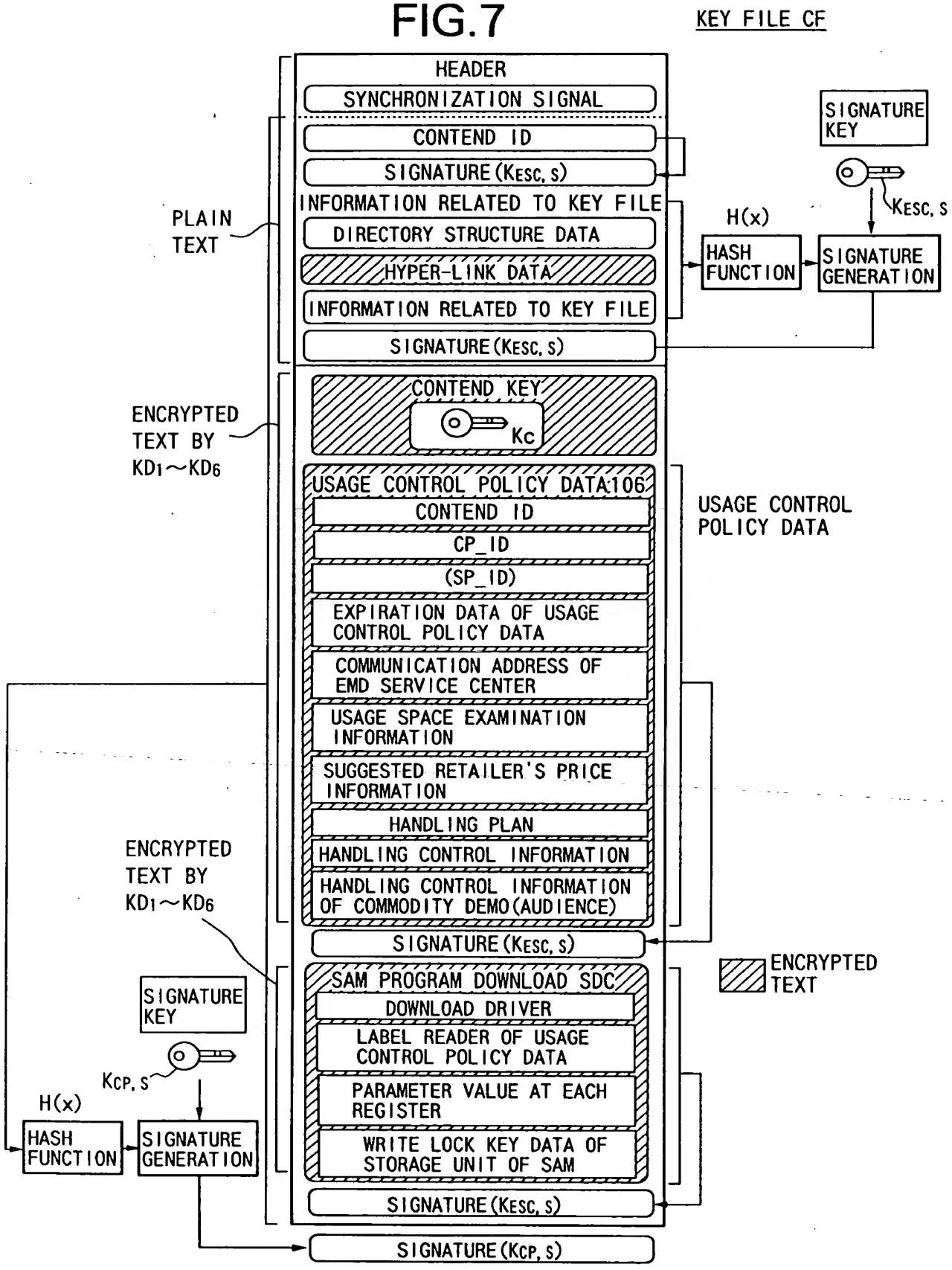

KEY FILE CF
HEADER
SYNCHRONIZATION SIGNAL
CONTEND ID
SIGNATURE (KESC, S)
INFORMATION RELATED TO KEY FILE
DIRECTORY STRUCTURE DATA
HYPER-LINK DATA
INFORMATION RELATED TO KEY FILE
SIGNATURE (KESC, S)
PLAIN TEXT
SIGNATURE KEY
KESC, S
H(x)
HASH FUNCTION
SIGNATURE GENERATION
CONTEND KEY
Kc
ENCRYPTED TEXT BY KD1~KD6
USAGE CONTROL POLICY DATA 106
CONTEND ID
CP_ID
(SP_ID)
EXPIRATION DATA OF USAGE CONTROL POLICY DATA
COMMUNICATION ADDRESS OF EMD SERVICE CENTER
USAGE SPACE EXAMINATION INFORMATION
SUGGESTED RETAILER'S PRICE INFORMATION
HANDLING PLAN
HANDLING CONTROL INFORMATION
HANDLING CONTROL INFORMATION OF COMMODITY DEMO (AUDIENCE)
USAGE CONTROL POLICY DATA
SIGNATURE (KESC, S)
ENCRYPTED TEXT BY KD1~KD6
ENCRYPTED TEXT
SAM PROGRAM DOWNLOAD SDC
DOWNLOAD DRIVER
LABEL READER OF USAGE CONTROL POLICY DATA
PARAMETER VALUE AT EACH REGISTER
WRITE LOCK KEY DATA OF STORAGE UNIT OF SAM
SIGNATURE (KESC, S)
SIGNATURE KEY
KCP, S
H(x)
HASH FUNCTION
SIGNATURE GENERATION
SIGNATURE (KCP, S)

FIG.8

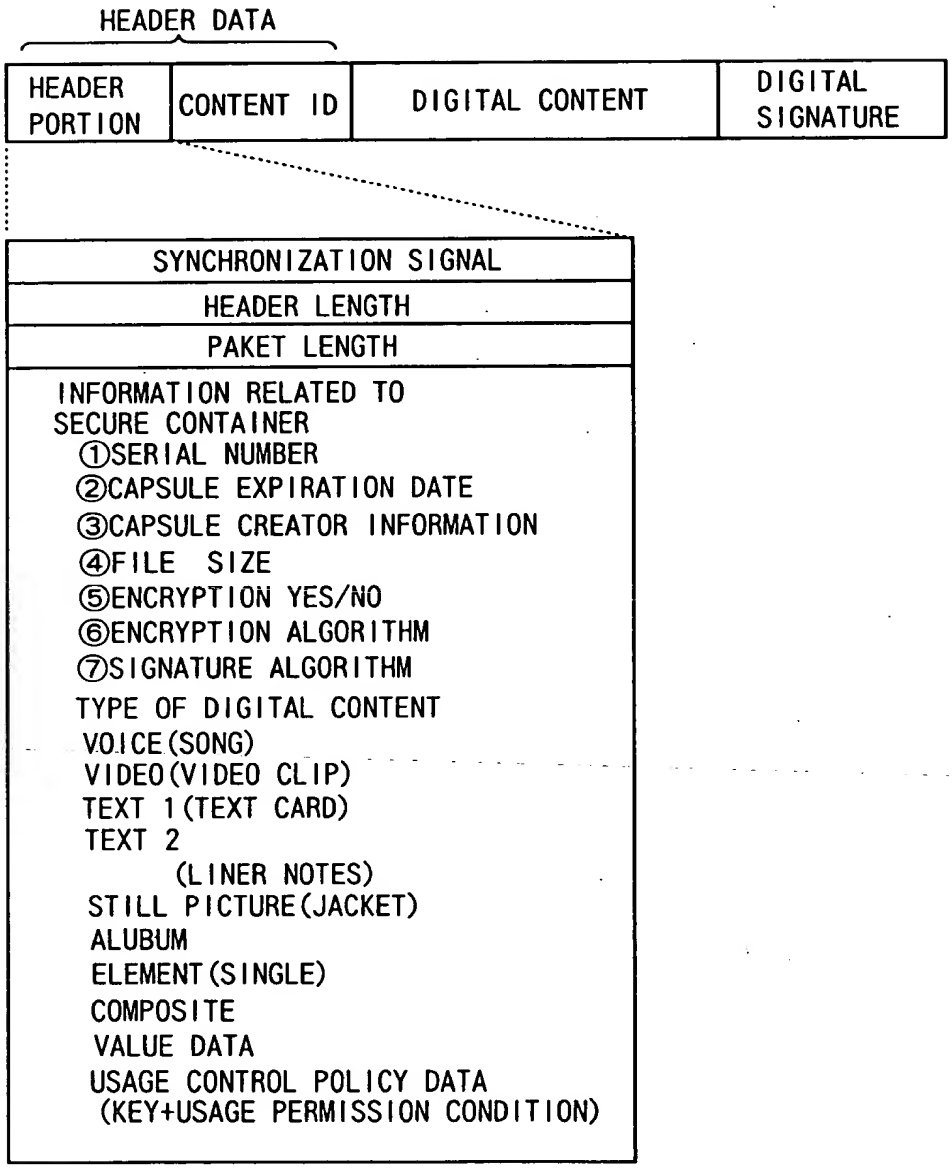


FIG.9

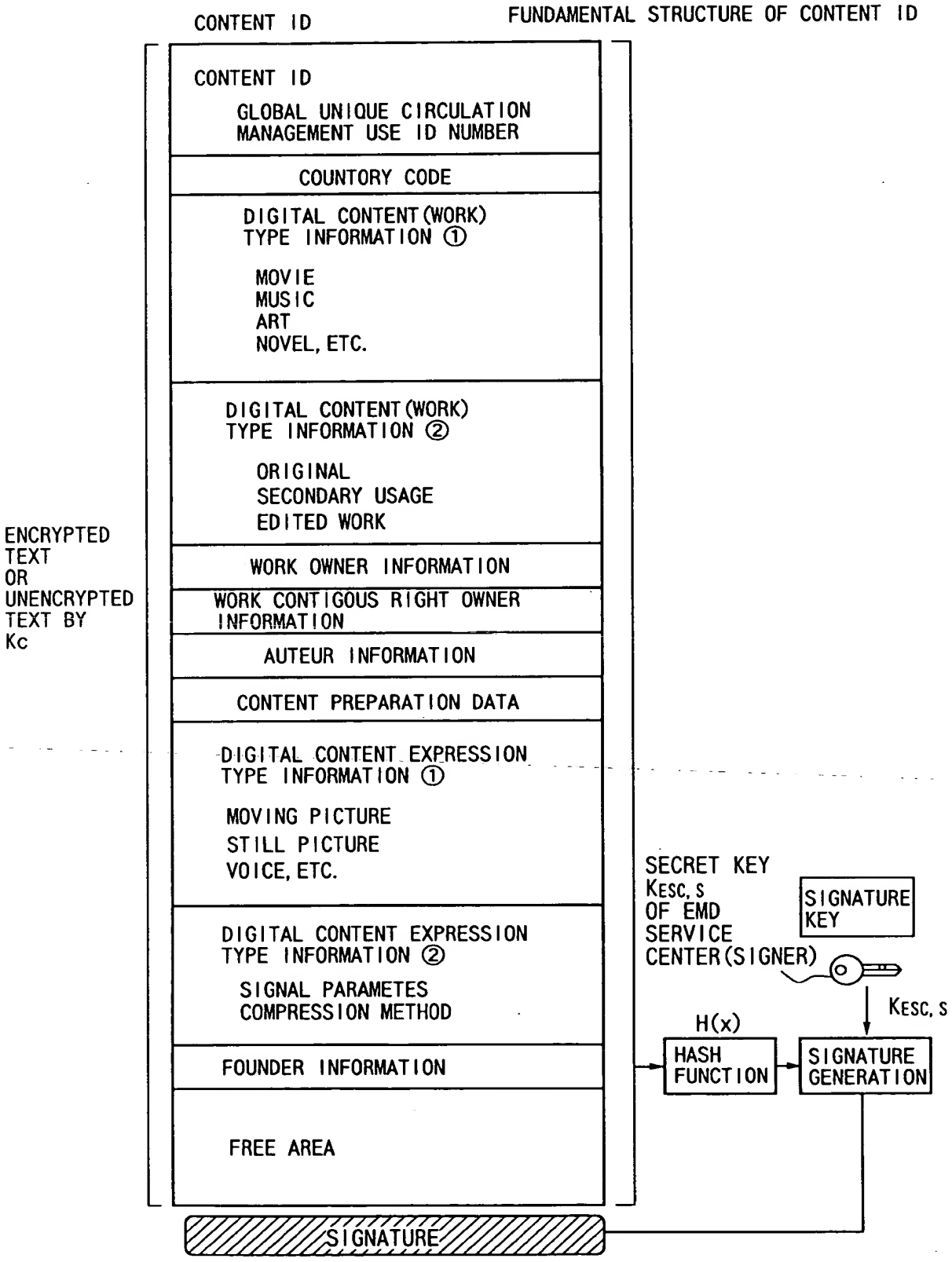

CONTENT ID
FUNDAMENTAL STRUCTURE OF CONTENT ID
CONTENT ID
GLOBAL UNIQUE CIRCULATION MANAGEMENT USE ID NUMBER
COUNTORY CODE
DIGITAL CONTENT(WORK) TYPE INFORMATION ①
MOVIE
MUSIC
ART
NOVEL, ETC.
DIGITAL CONTENT(WORK) TYPE INFORMATION ②
ORIGINAL
SECONDARY USAGE
EDITED WORK
WORK OWNER INFORMATION
WORK CONTIGOUS RIGHT OWNER INFORMATION
AUTEUR INFORMATION
CONTENT PREPARATION DATA
DIGITAL CONTENT EXPRESSION TYPE INFORMATION ①
MOVING PICTURE
STILL PICTURE
VOICE, ETC.
DIGITAL CONTENT EXPRESSION TYPE INFORMATION ②
SIGNAL PARAMETES
COMPRESSION METHOD
FOUNDER INFORMATION
FREE AREA
SIGNATURE
ENCRYPTED TEXT OR UNENCRYPTED TEXT BY Kc
SECRET KEY KESC, S OF EMD SERVICE CENTER(SIGNER)
SIGNATURE KEY
KESC, S
H(x)
HASH FUNCTION
SIGNATURE GENERATION

FIG.10

DIRECTORY STRUCTURE OF SECURE CONTAINER

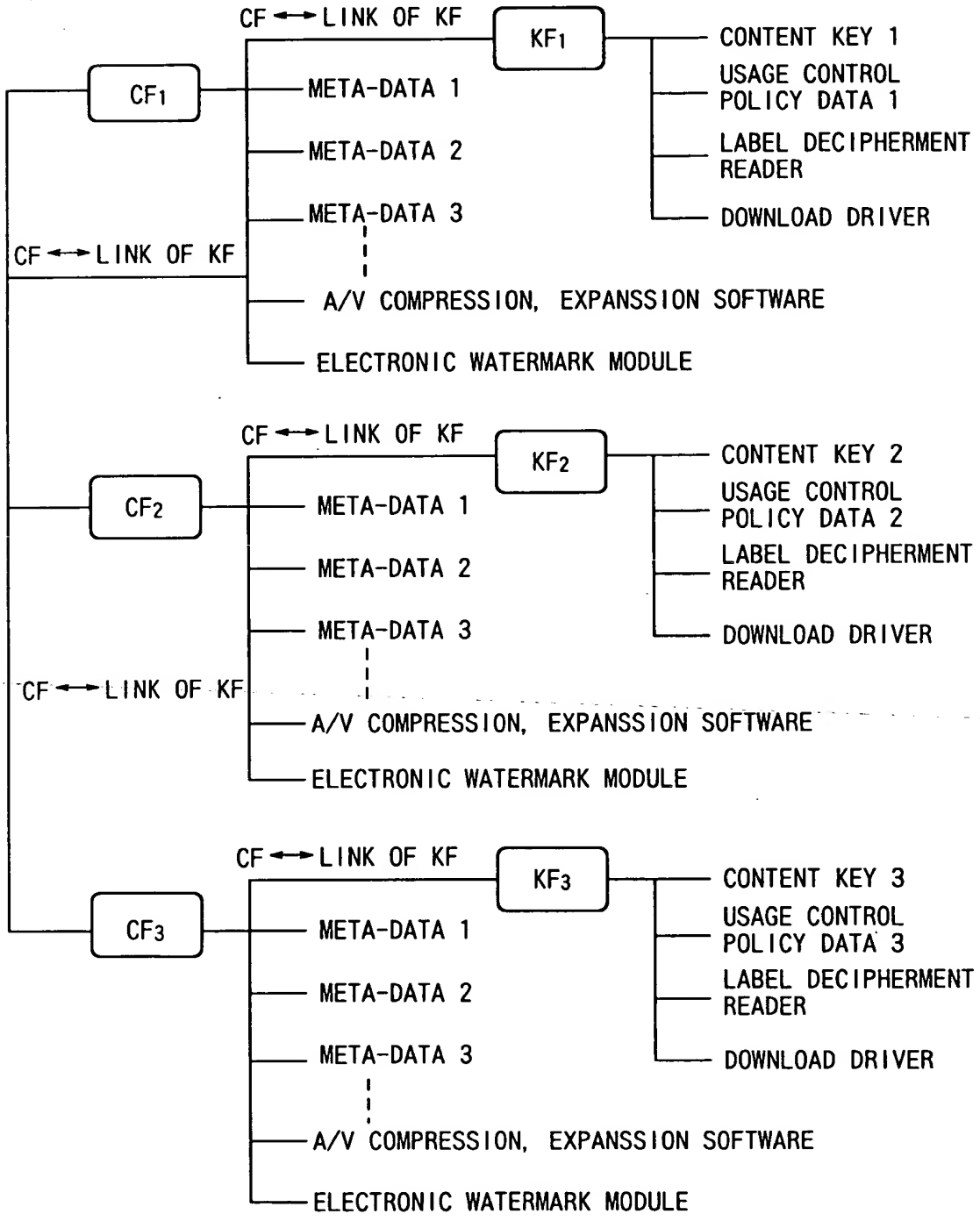


FIG.11

HYPER-LINK DATA OF SECURE CONTAINER

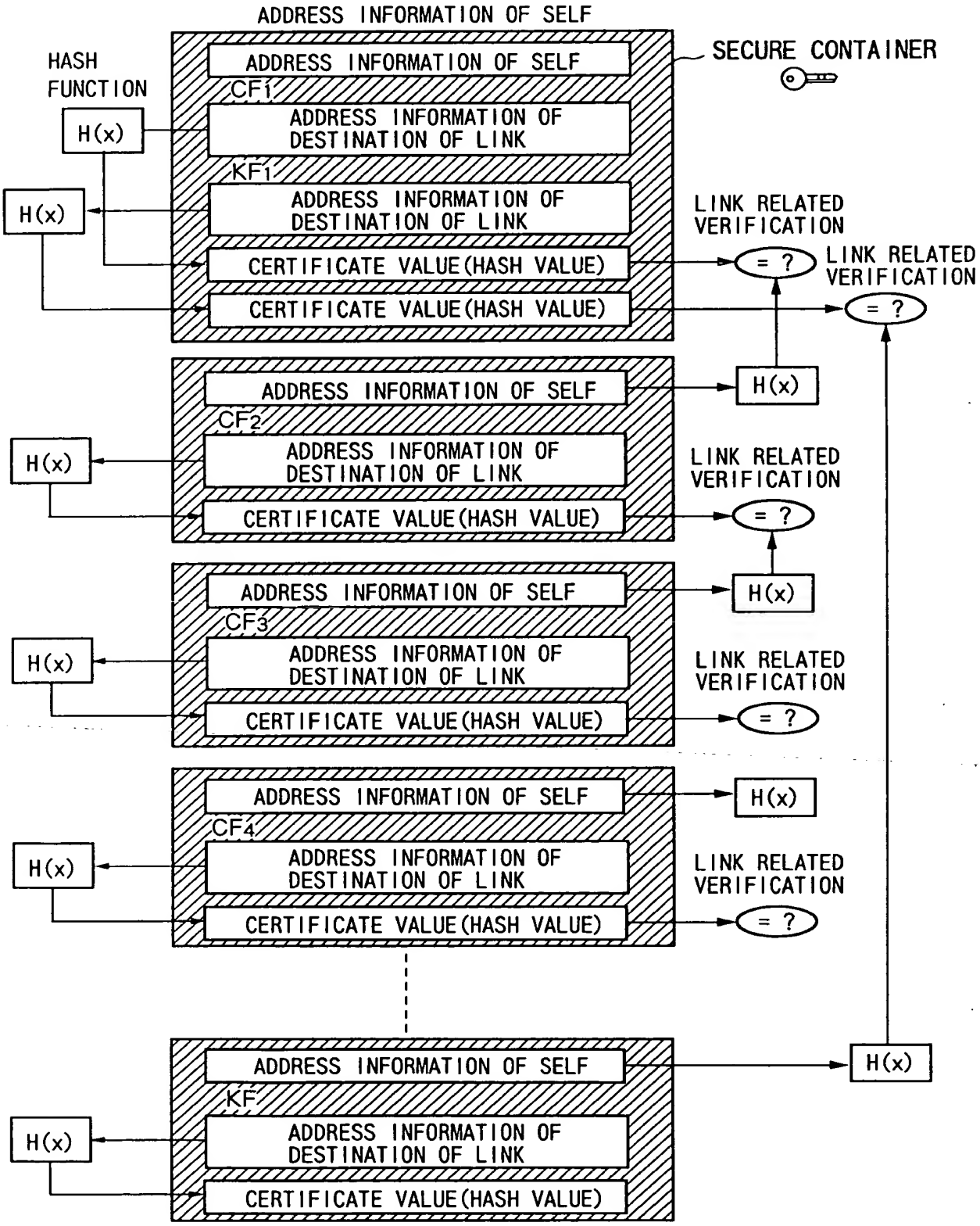


FIG.12

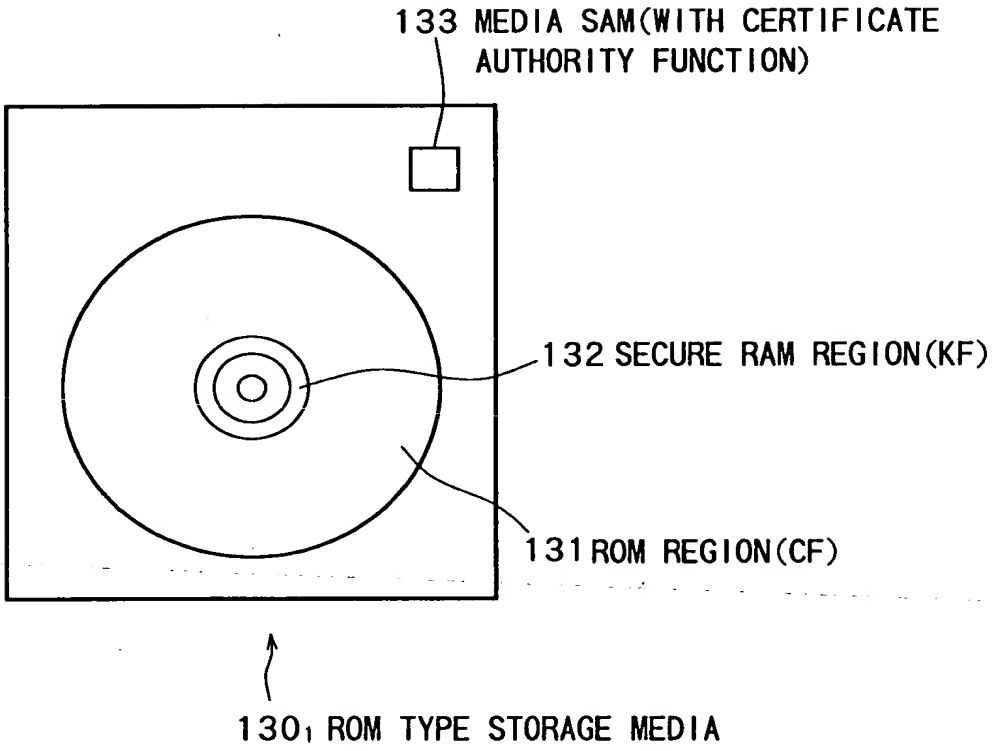


FIG.13

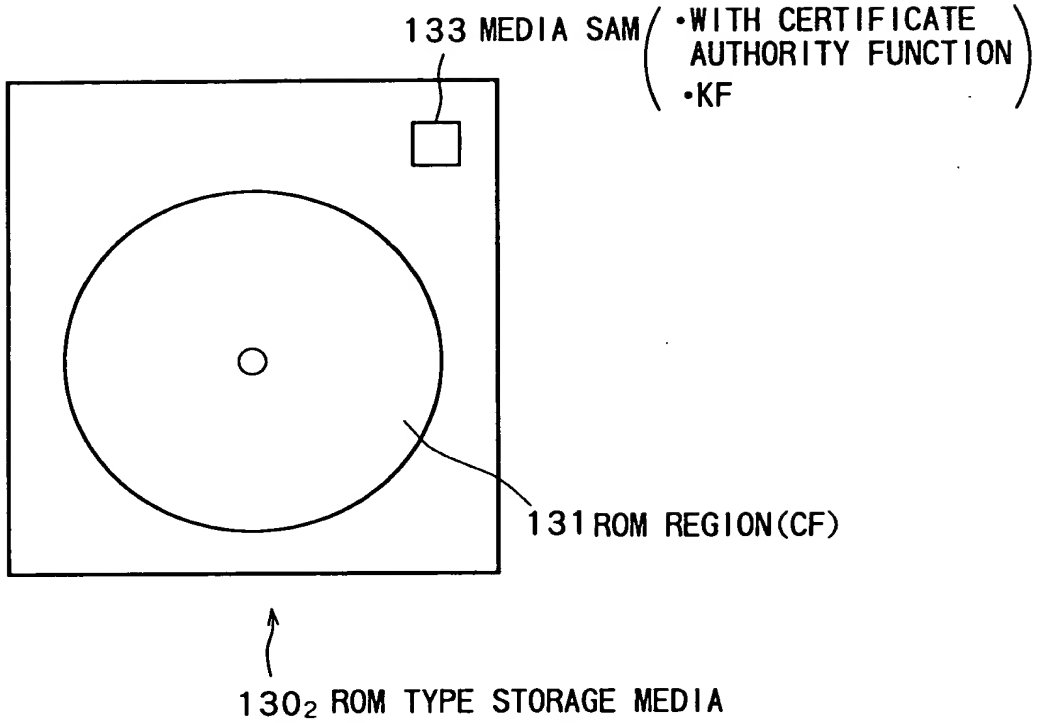

133 MEDIA SAM
•WITH CERTIFICATE AUTHORITY FUNCTION
•KF
131 ROM REGION(CF)
130$_2$ ROM TYPE STORAGE MEDIA

FIG.14

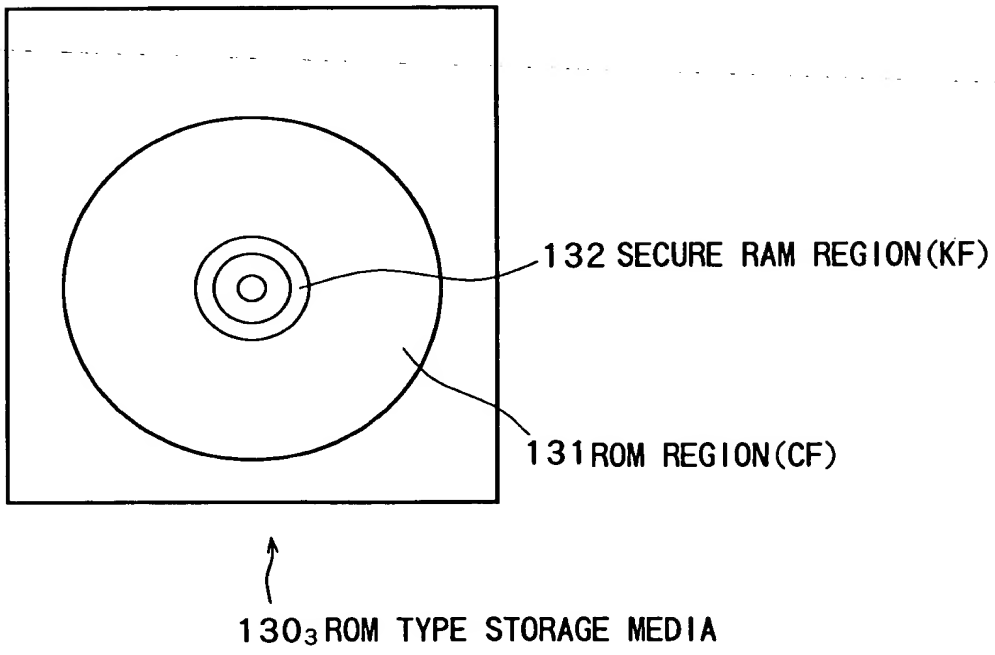

132 SECURE RAM REGION(KF)
131 ROM REGION(CF)
130$_3$ ROM TYPE STORAGE MEDIA

FIG.15

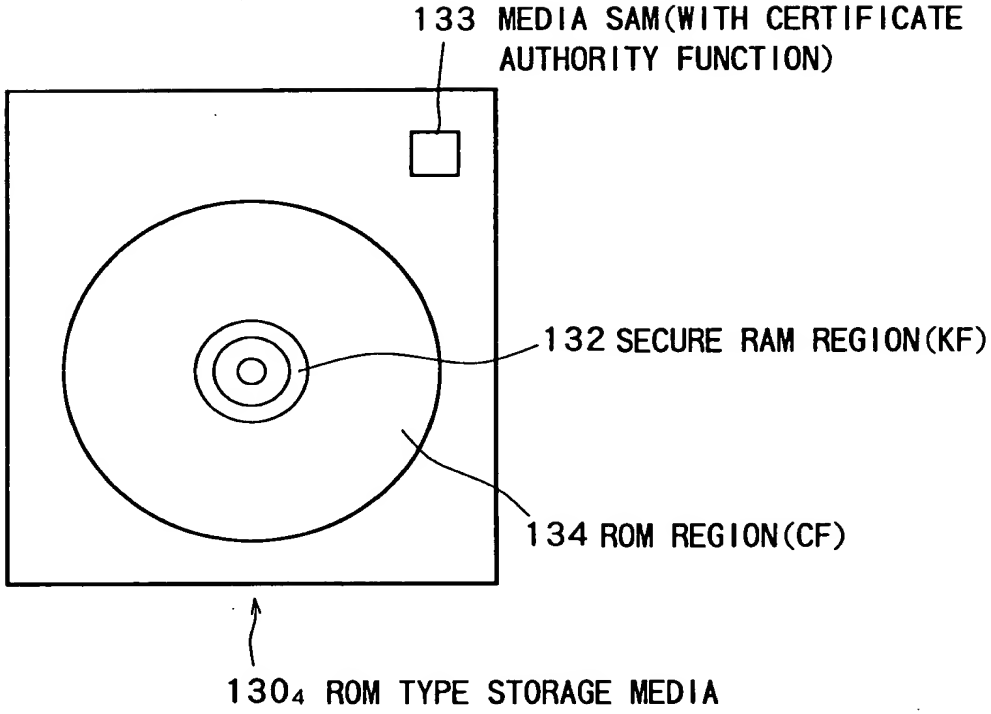

133 MEDIA SAM(WITH CERTIFICATE AUTHORITY FUNCTION)
132 SECURE RAM REGION(KF)
134 ROM REGION(CF)
130₄ ROM TYPE STORAGE MEDIA

FIG.16

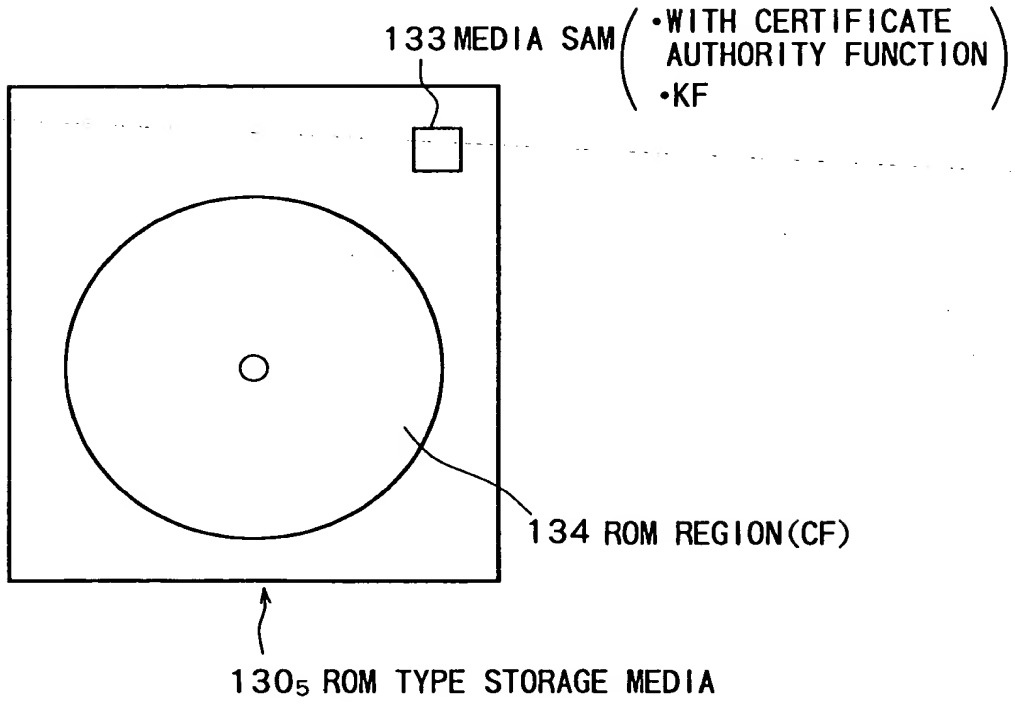

133 MEDIA SAM (•WITH CERTIFICATE AUTHORITY FUNCTION •KF)
134 ROM REGION(CF)
130₅ ROM TYPE STORAGE MEDIA

FIG.17

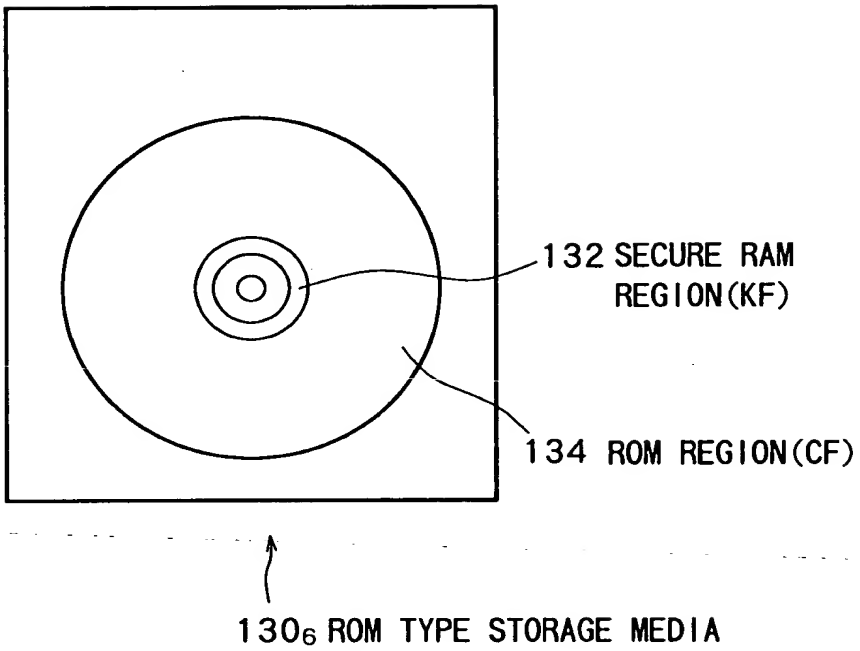


FIG.18

CONTENT PROVIDER
101
KEY FILE KF
×6 MONTHS' WORTH
EMD SERVICE CENTER
102
REGISTRATION USE MODULE Mod2
$K_{CP,S}$
$SIG_{M1,CP}$
CONTENT ID
CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA 106
ELECTONIC WATERMARK INFORMATION
MANAGEMENT DATA WM
CP_ID
SP_ID
SRD

FIG.19

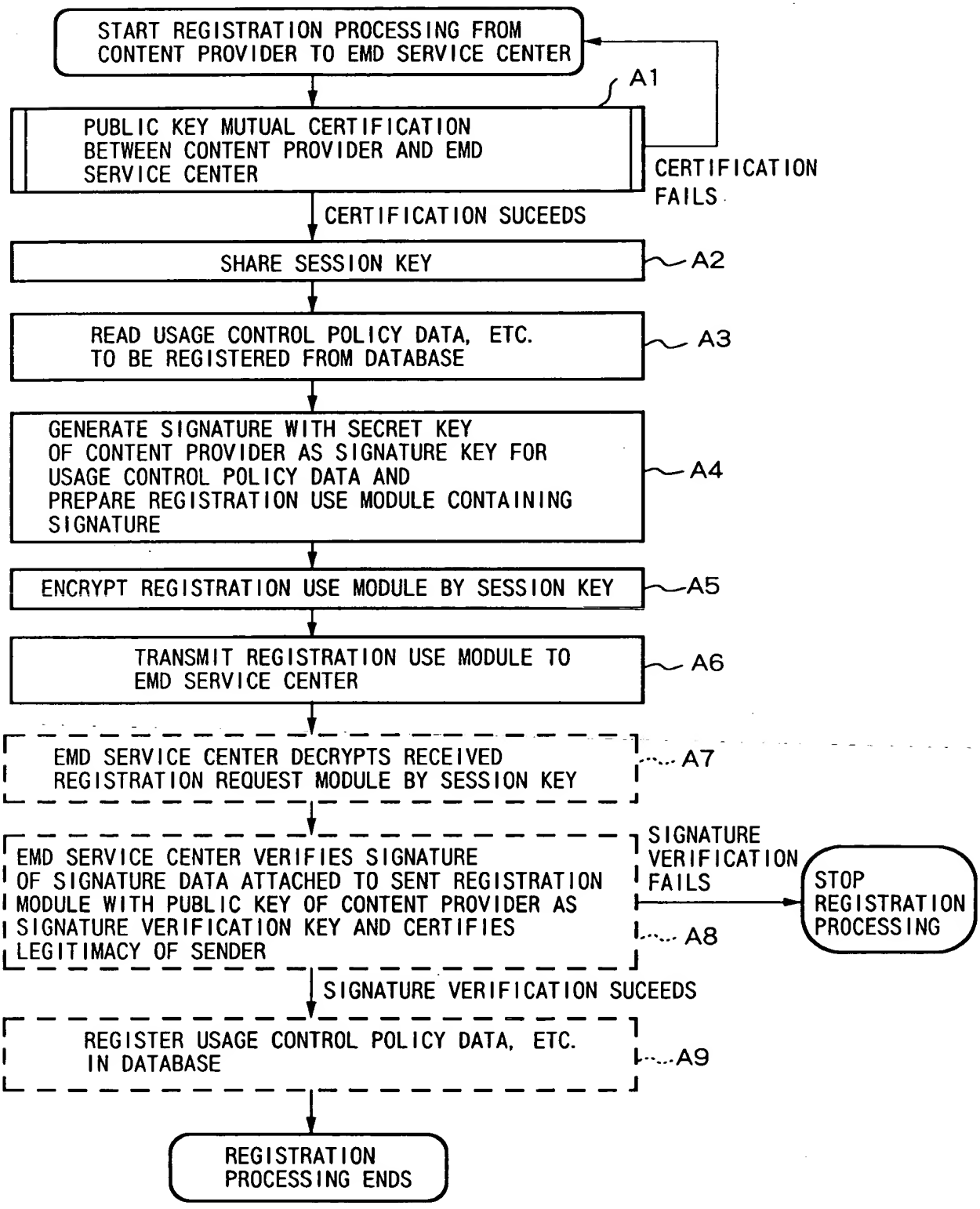

START REGISTRATION PROCESSING FROM CONTENT PROVIDER TO EMD SERVICE CENTER
A1
PUBLIC KEY MUTUAL CERTIFICATION BETWEEN CONTENT PROVIDER AND EMD SERVICE CENTER
CERTIFICATION FAILS
CERTIFICATION SUCEEDS
SHARE SESSION KEY
A2
READ USAGE CONTROL POLICY DATA, ETC. TO BE REGISTERED FROM DATABASE
A3
GENERATE SIGNATURE WITH SECRET KEY OF CONTENT PROVIDER AS SIGNATURE KEY FOR USAGE CONTROL POLICY DATA AND PREPARE REGISTRATION USE MODULE CONTAINING SIGNATURE
A4
ENCRYPT REGISTRATION USE MODULE BY SESSION KEY
A5
TRANSMIT REGISTRATION USE MODULE TO EMD SERVICE CENTER
A6
EMD SERVICE CENTER DECRYPTS RECEIVED REGISTRATION REQUEST MODULE BY SESSION KEY
A7
EMD SERVICE CENTER VERIFIES SIGNATURE OF SIGNATURE DATA ATTACHED TO SENT REGISTRATION MODULE WITH PUBLIC KEY OF CONTENT PROVIDER AS SIGNATURE VERIFICATION KEY AND CERTIFIES LEGITIMACY OF SENDER
A8
SIGNATURE VERIFICATION FAILS
STOP REGISTRATION PROCESSING
SIGNATURE VERIFICATION SUCEEDS
REGISTER USAGE CONTROL POLICY DATA, ETC. IN DATABASE
A9
REGISTRATION PROCESSING ENDS

FIG.20

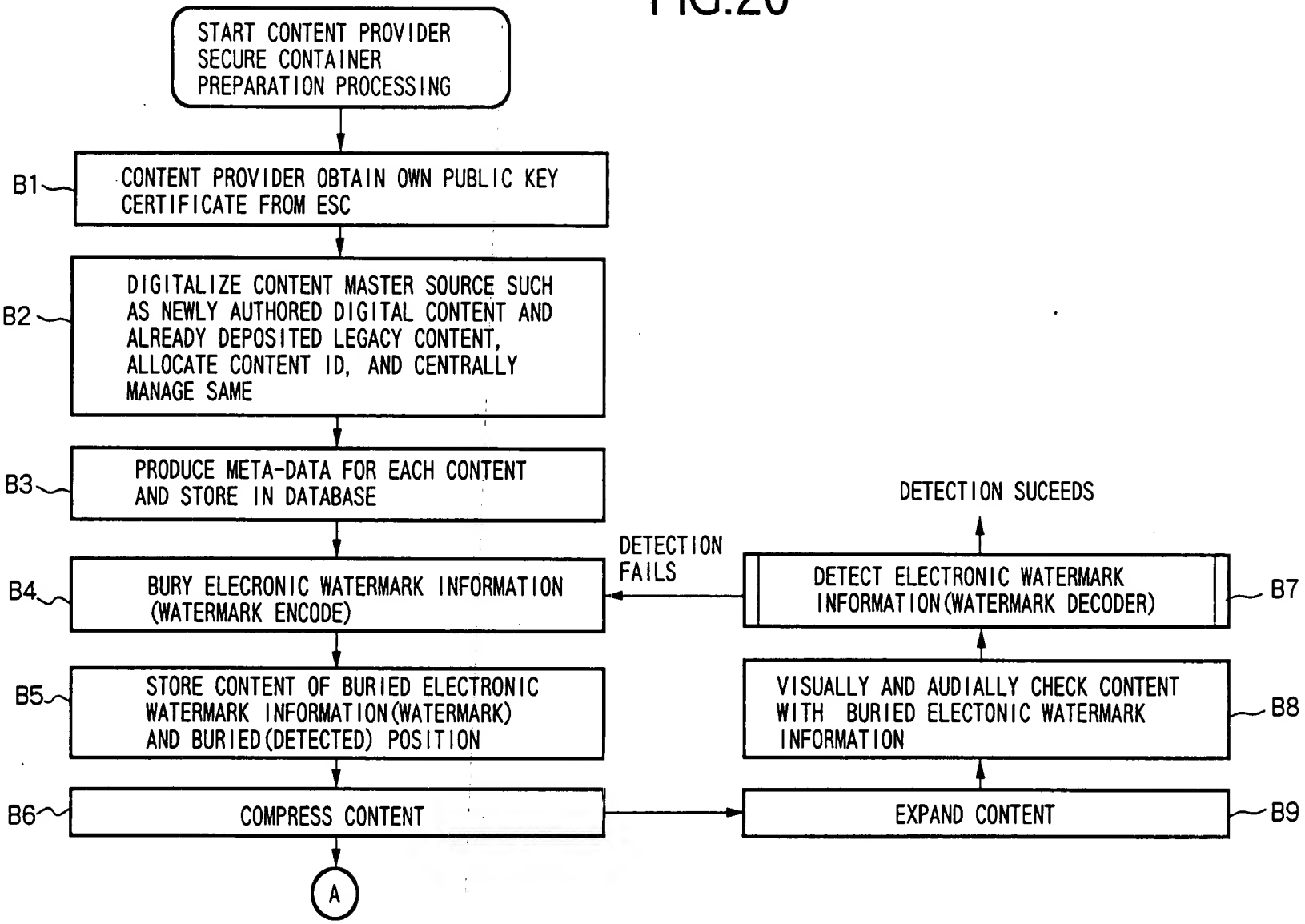


FIG.21

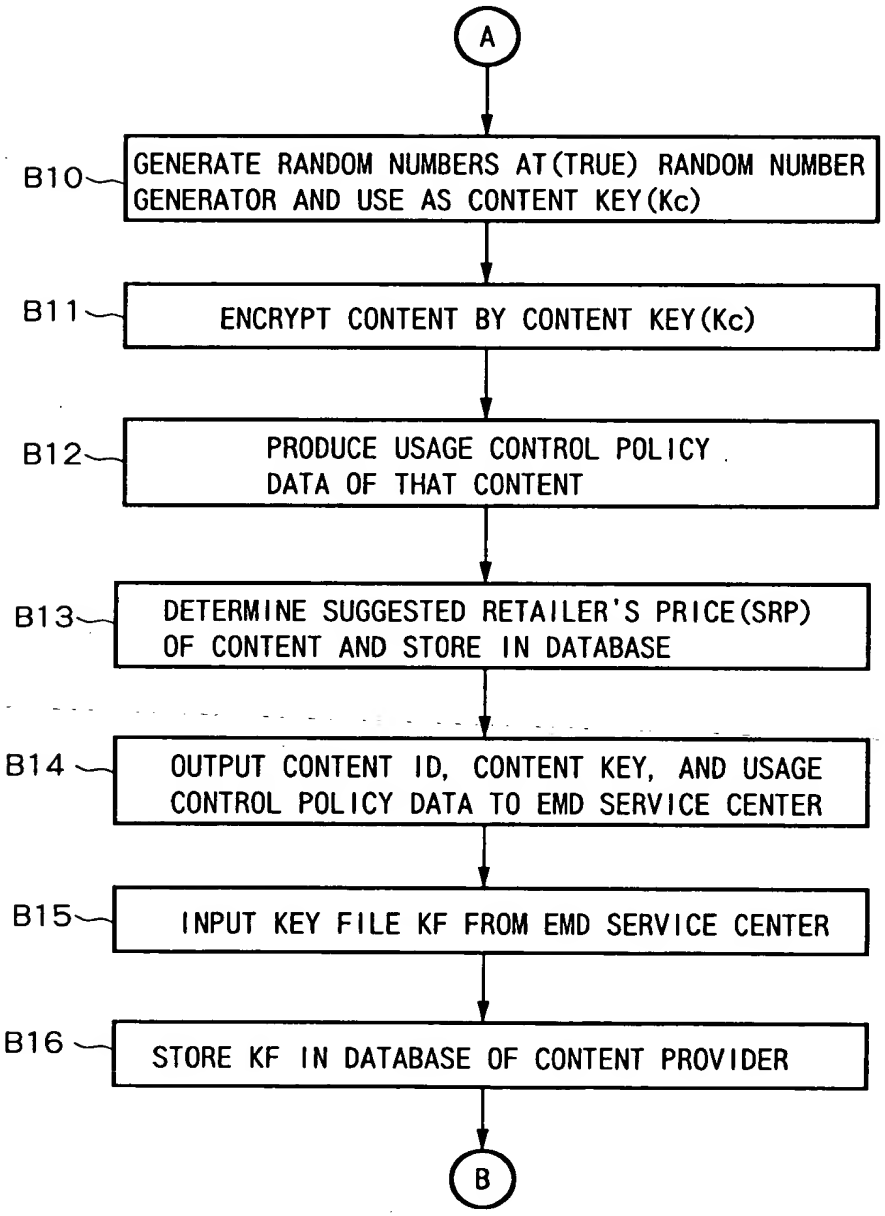

A
B10
GENERATE RANDOM NUMBERS AT(TRUE) RANDOM NUMBER GENERATOR AND USE AS CONTENT KEY(Kc)
B11
ENCRYPT CONTENT BY CONTENT KEY(Kc)
B12
PRODUCE USAGE CONTROL POLICY DATA OF THAT CONTENT
B13
DETERMINE SUGGESTED RETAILER'S PRICE(SRP) OF CONTENT AND STORE IN DATABASE
B14
OUTPUT CONTENT ID, CONTENT KEY, AND USAGE CONTROL POLICY DATA TO EMD SERVICE CENTER
B15
INPUT KEY FILE KF FROM EMD SERVICE CENTER
B16
STORE KF IN DATABASE OF CONTENT PROVIDER
B

FIG.22

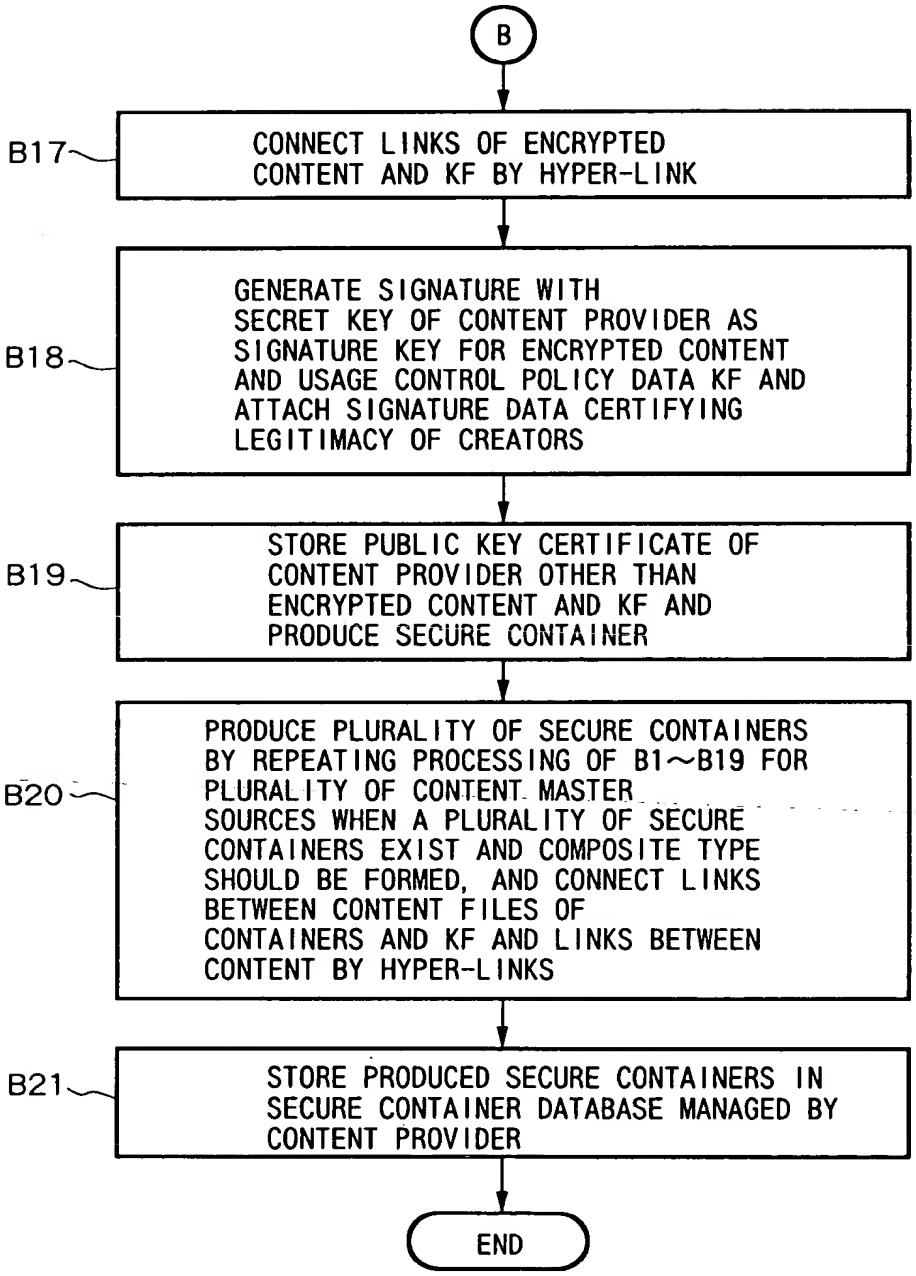

B
B17
CONNECT LINKS OF ENCRYPTED CONTENT AND KF BY HYPER-LINK
B18
GENERATE SIGNATURE WITH SECRET KEY OF CONTENT PROVIDER AS SIGNATURE KEY FOR ENCRYPTED CONTENT AND USAGE CONTROL POLICY DATA KF AND ATTACH SIGNATURE DATA CERTIFYING LEGITIMACY OF CREATORS
B19
STORE PUBLIC KEY CERTIFICATE OF CONTENT PROVIDER OTHER THAN ENCRYPTED CONTENT AND KF AND PRODUCE SECURE CONTAINER
B20
PRODUCE PLURALITY OF SECURE CONTAINERS BY REPEATING PROCESSING OF B1~B19 FOR PLURALITY OF CONTENT MASTER SOURCES WHEN A PLURALITY OF SECURE CONTAINERS EXIST AND COMPOSITE TYPE SHOULD BE FORMED, AND CONNECT LINKS BETWEEN CONTENT FILES OF CONTAINERS AND KF AND LINKS BETWEEN CONTENT BY HYPER-LINKS
B21
STORE PRODUCED SECURE CONTAINERS IN SECURE CONTAINER DATABASE MANAGED BY CONTENT PROVIDER
END

FIG.23

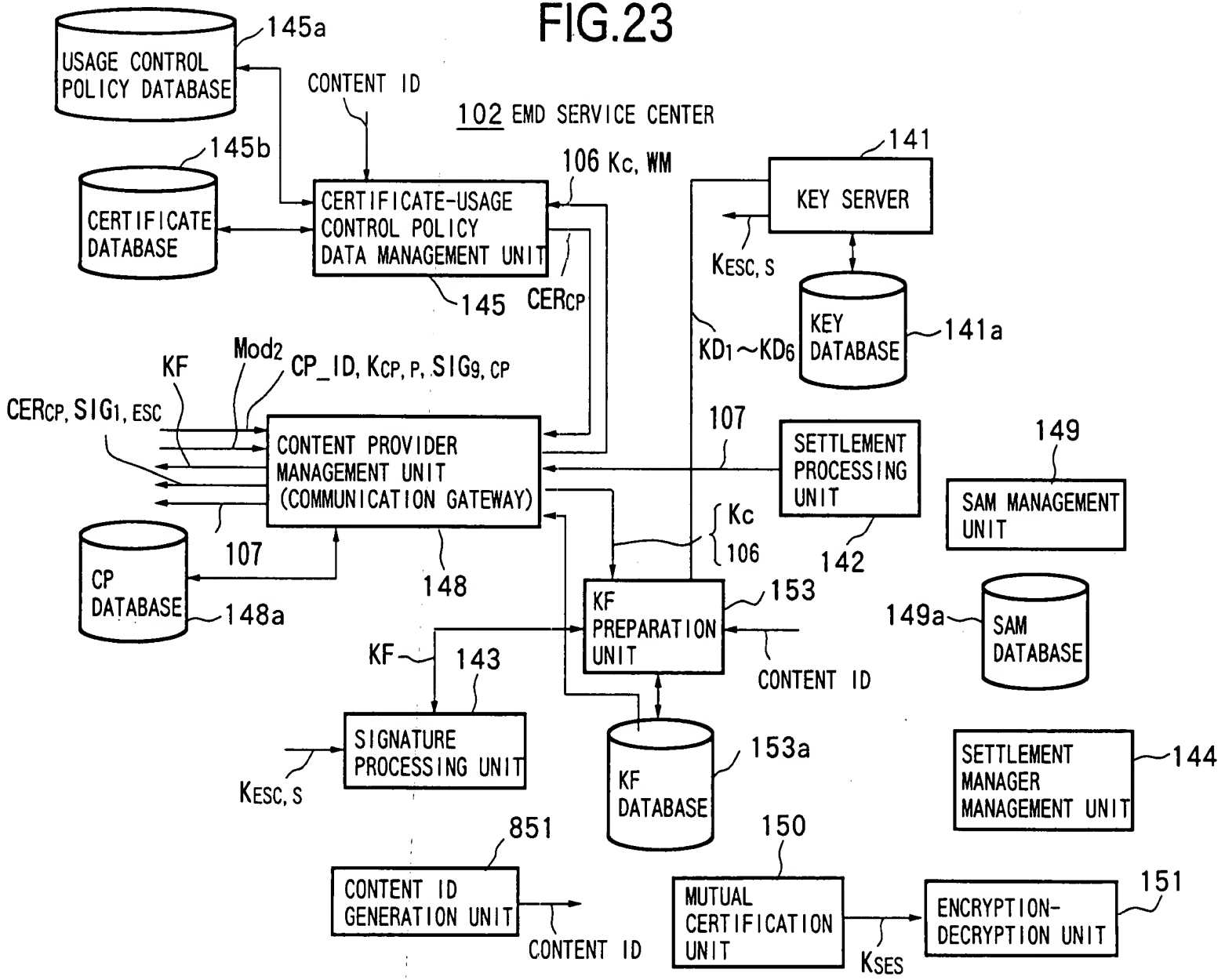


FIG.24

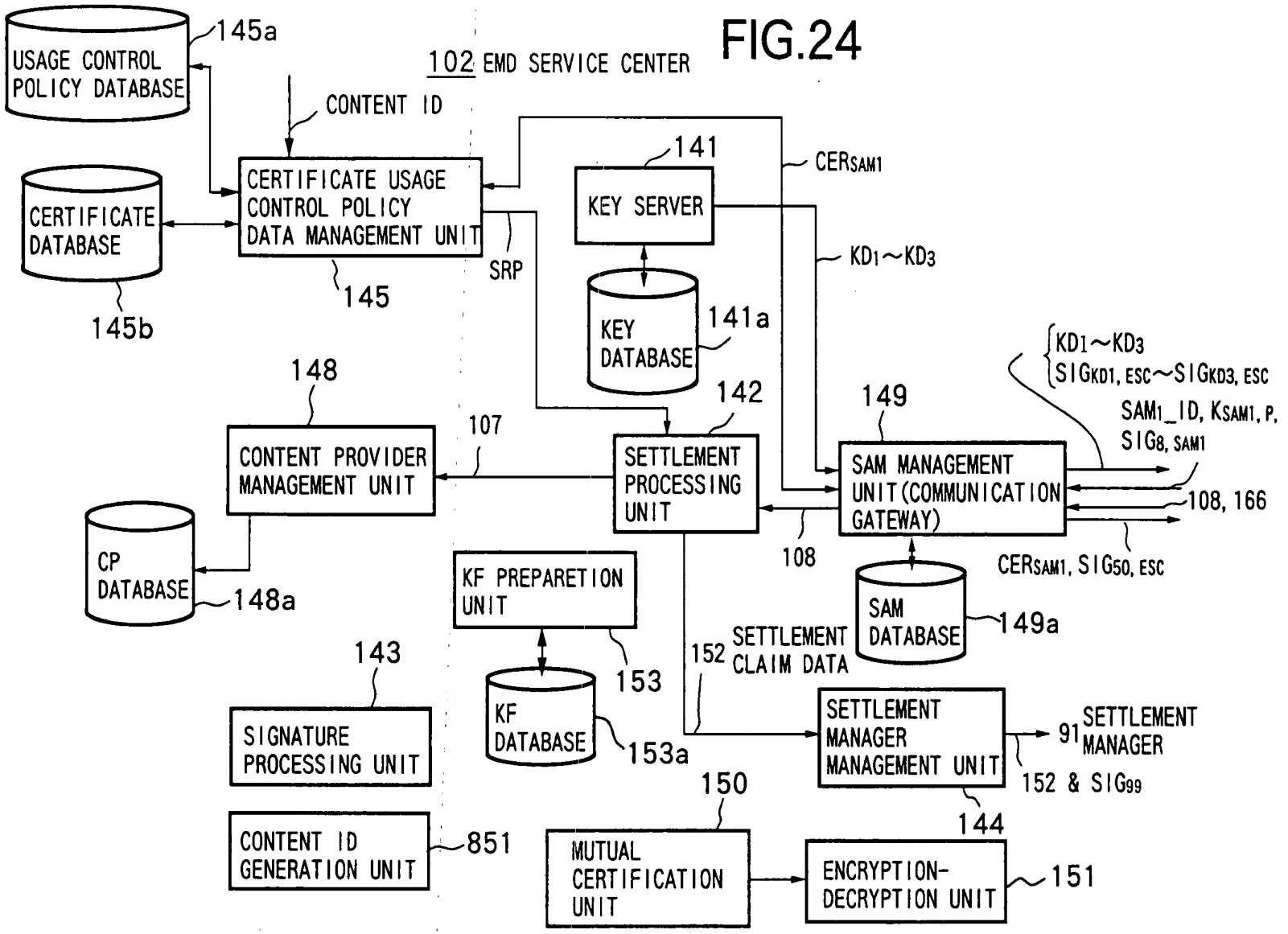

USAGE CONTROL POLICY DATABASE
145a
102 EMD SERVICE CENTER
CONTENT ID
CERTIFICATE USAGE CONTROL POLICY DATA MANAGEMENT UNIT
CERTIFICATE DATABASE
145b
145
SRP
141
KEY SERVER
CERSAM1
KD1~KD3
KEY DATABASE
141a
148
CONTENT PROVIDER MANAGEMENT UNIT
107
142
SETTLEMENT PROCESSING UNIT
149
SAM MANAGEMENT UNIT (COMMUNICATION GATEWAY)
KD1~KD3
SIGKD1, ESC~SIGKD3, ESC
SAM1_ID, KSAM1, P, SIG8, SAM1
108, 166
CERSAM1, SIG50, ESC
108
CP DATABASE
148a
KF PREPARETION UNIT
153
KF DATABASE
153a
SAM DATABASE
149a
152 SETTLEMENT CLAIM DATA
143
SIGNATURE PROCESSING UNIT
SETTLEMENT MANAGER MANAGEMENT UNIT
91 SETTLEMENT MANAGER
152 & SIG99
150
144
CONTENT ID GENERATION UNIT
851
MUTUAL CERTIFICATION UNIT
ENCRYPTION-DECRYPTION UNIT
151

FIG.25

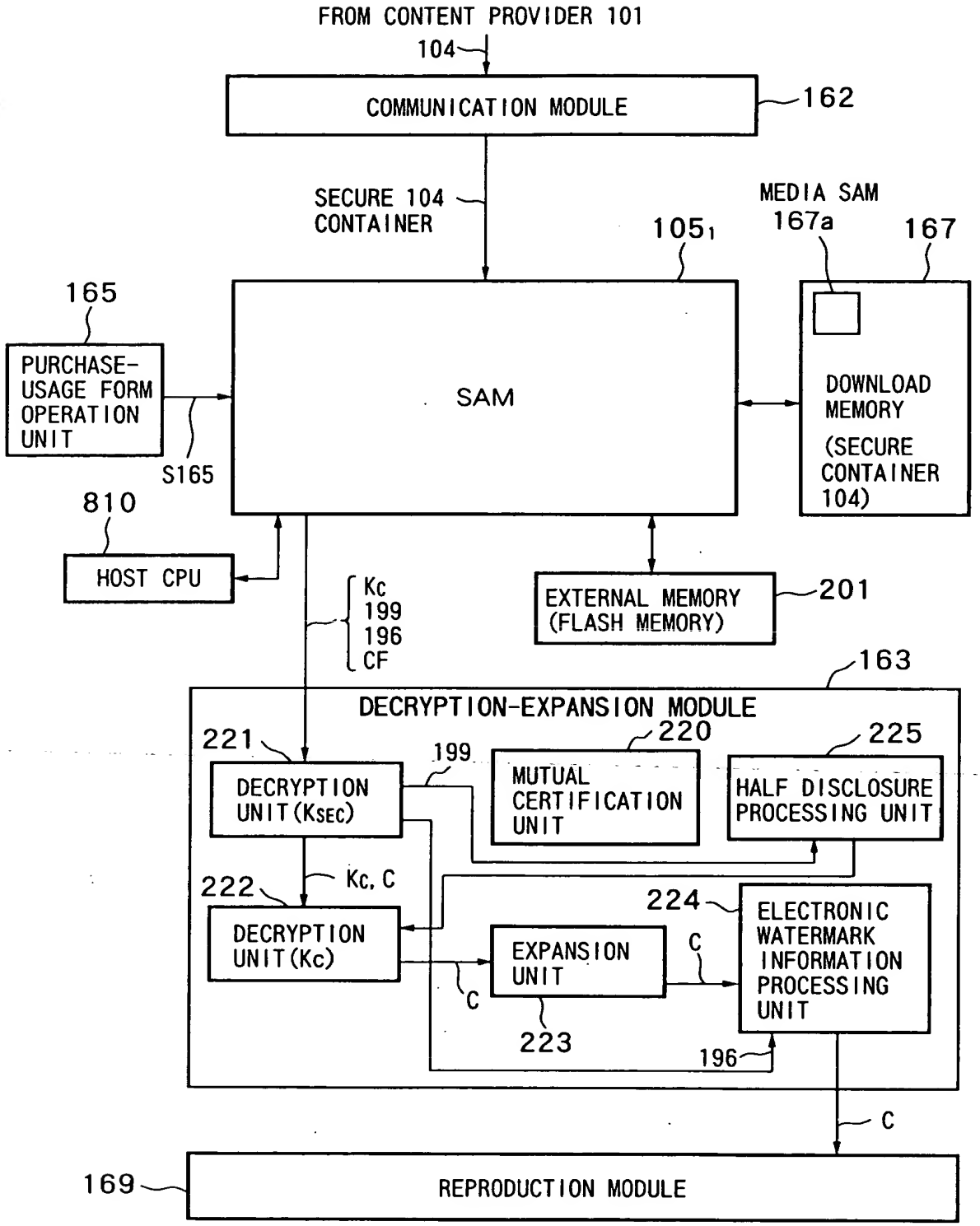

FROM CONTENT PROVIDER 101
104
COMMUNICATION MODULE
162
SECURE 104 CONTAINER
MEDIA SAM
167a
167
105₁
165
PURCHASE-USAGE FORM OPERATION UNIT
SAM
DOWNLOAD MEMORY
(SECURE CONTAINER 104)
S165
810
HOST CPU
Kc
199
196
CF
EXTERNAL MEMORY (FLASH MEMORY)
201
163
DECRYPTION-EXPANSION MODULE
221
220
225
199
DECRYPTION UNIT(Ksec)
MUTUAL CERTIFICATION UNIT
HALF DISCLOSURE PROCESSING UNIT
Kc, C
222
224
DECRYPTION UNIT(Kc)
EXPANSION UNIT
C
ELECTRONIC WATERMARK INFORMATION PROCESSING UNIT
C
223
196
C
169
REPRODUCTION MODULE

FIG.26

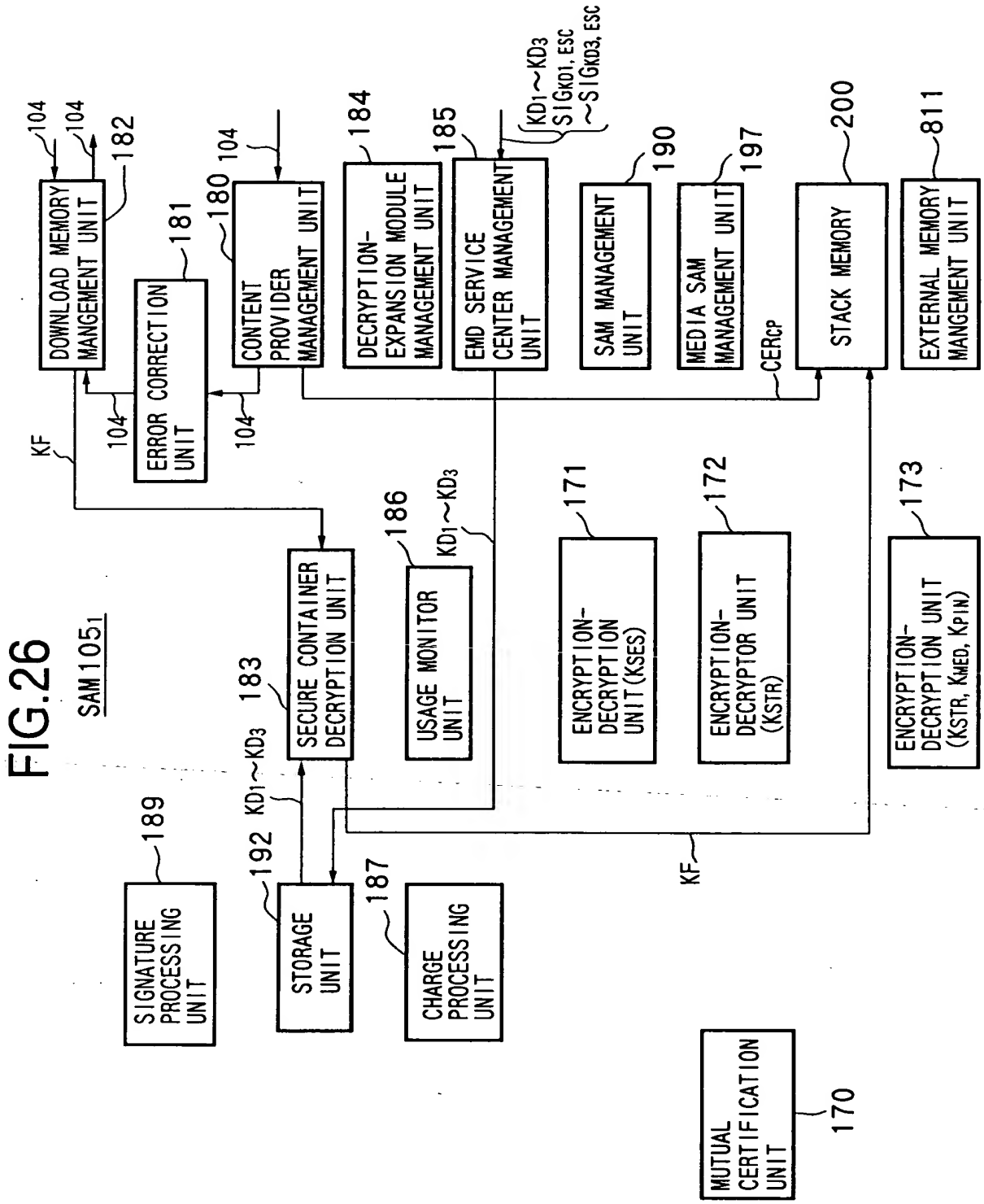

SAM 105₁
DOWNLOAD MEMORY MANGEMENT UNIT
182
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
SAM MANAGEMENT UNIT
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANGEMENT UNIT
811
SECURE CONTAINER DECRYPTION UNIT
183
USAGE MONITOR UNIT
186
ENCRYPTION-DECRYPTION UNIT (KSES)
171
ENCRYPTION-DECRYPTOR UNIT (KSTR)
172
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
173
SIGNATURE PROCESSING UNIT
189
STORAGE UNIT
192
CHARGE PROCESSING UNIT
187
MUTUAL CERTIFICATION UNIT
170
KF
KD1~KD3
SIGKD1, ESC
~SIGKD3, ESC
CERCP
104

FIG.27

DATA STORED IN EXTERNAL MEMORY 201

USAGE LOG DATA 108
SAM REGISTRATION LIST

FIG.28

DATA STORED IN STACK MEMORY 200

CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA(USP) 106
LOCK KEY DATA K_{LOG} OF STORAGE UNIT(FLASH MEMORY) 192
CERTIFICATE CER_{CP} OF CONTENT PROVIDER 101
USAGE CONTROL STATUS DATA(UCS) 166
SAM PROGRAM DOWNLORD CONTAINERS SD_1 TO SDC_3

FIG.29

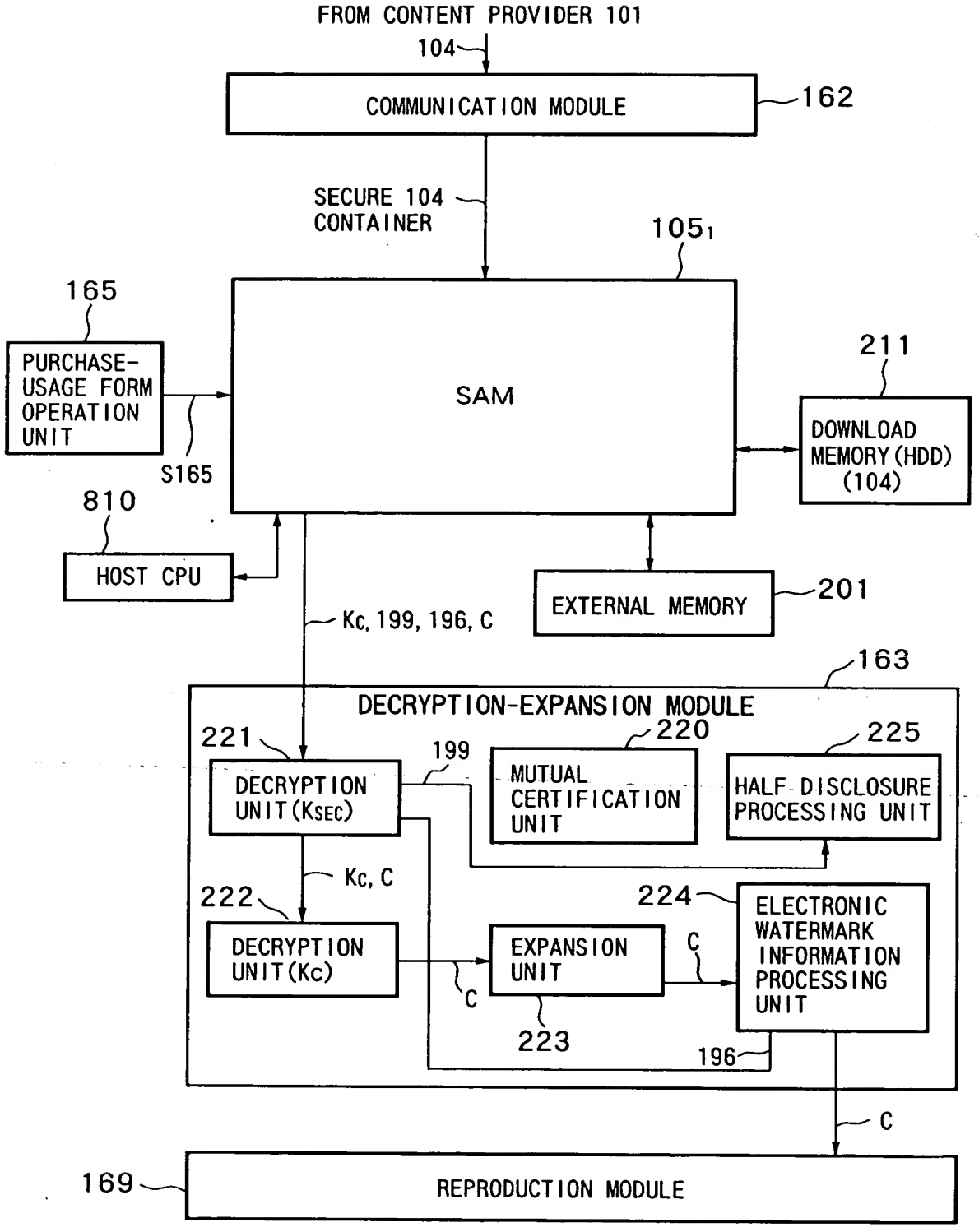

FROM CONTENT PROVIDER 101
104
COMMUNICATION MODULE
162
SECURE 104 CONTAINER
105₁
165
PURCHASE-USAGE FORM OPERATION UNIT
S165
SAM
211
DOWNLOAD MEMORY (HDD) (104)
810
HOST CPU
EXTERNAL MEMORY
201
Kc, 199, 196, C
163
DECRYPTION-EXPANSION MODULE
221
DECRYPTION UNIT (KSEC)
199
220
MUTUAL CERTIFICATION UNIT
225
HALF-DISCLOSURE PROCESSING UNIT
Kc, C
222
DECRYPTION UNIT (Kc)
C
EXPANSION UNIT
223
224
ELECTRONIC WATERMARK INFORMATION PROCESSING UNIT
C
196
C
169
REPRODUCTION MODULE

FIG.30

DATA STORED IN STORAGE UNIT 192

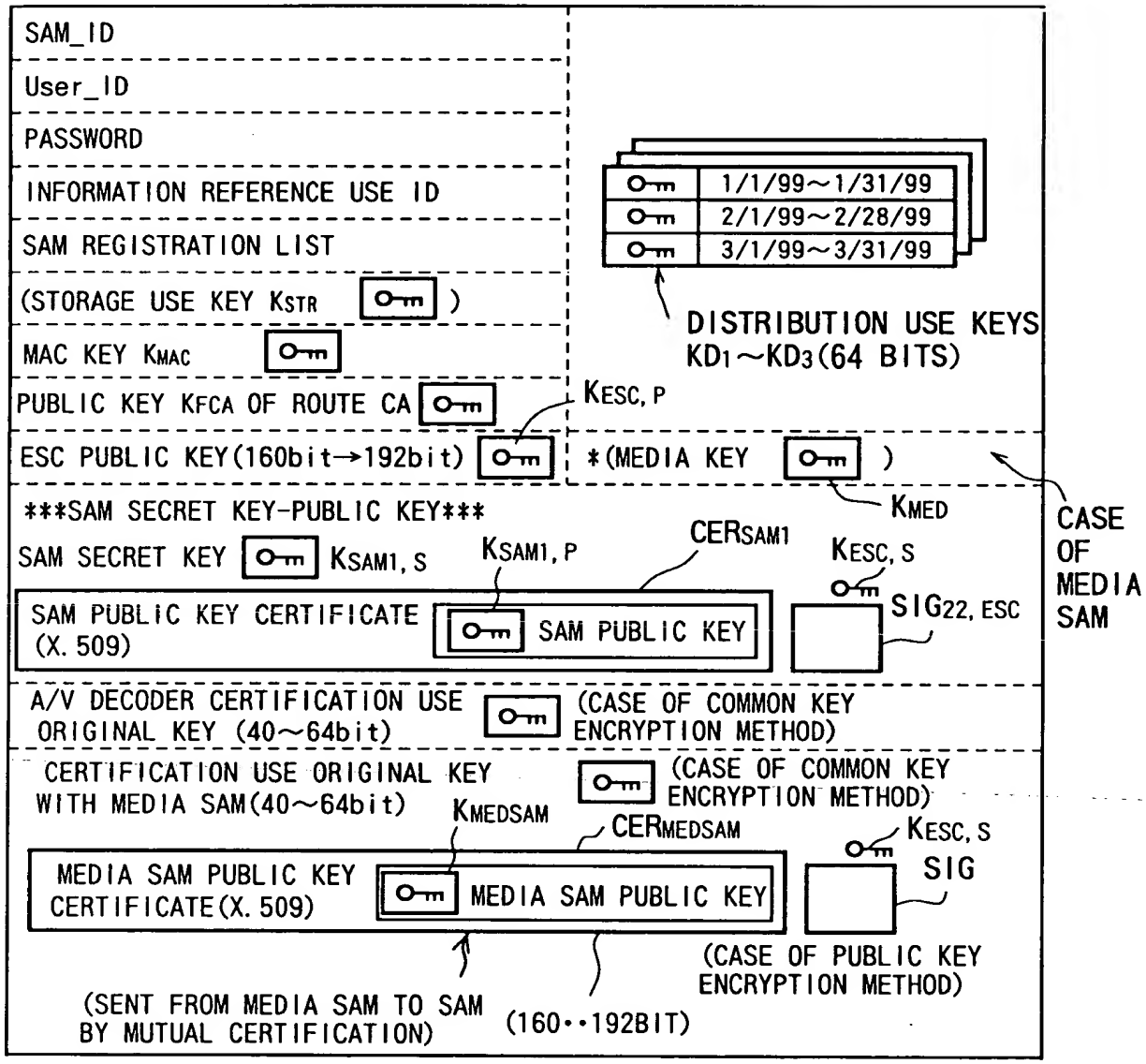


FIG.31

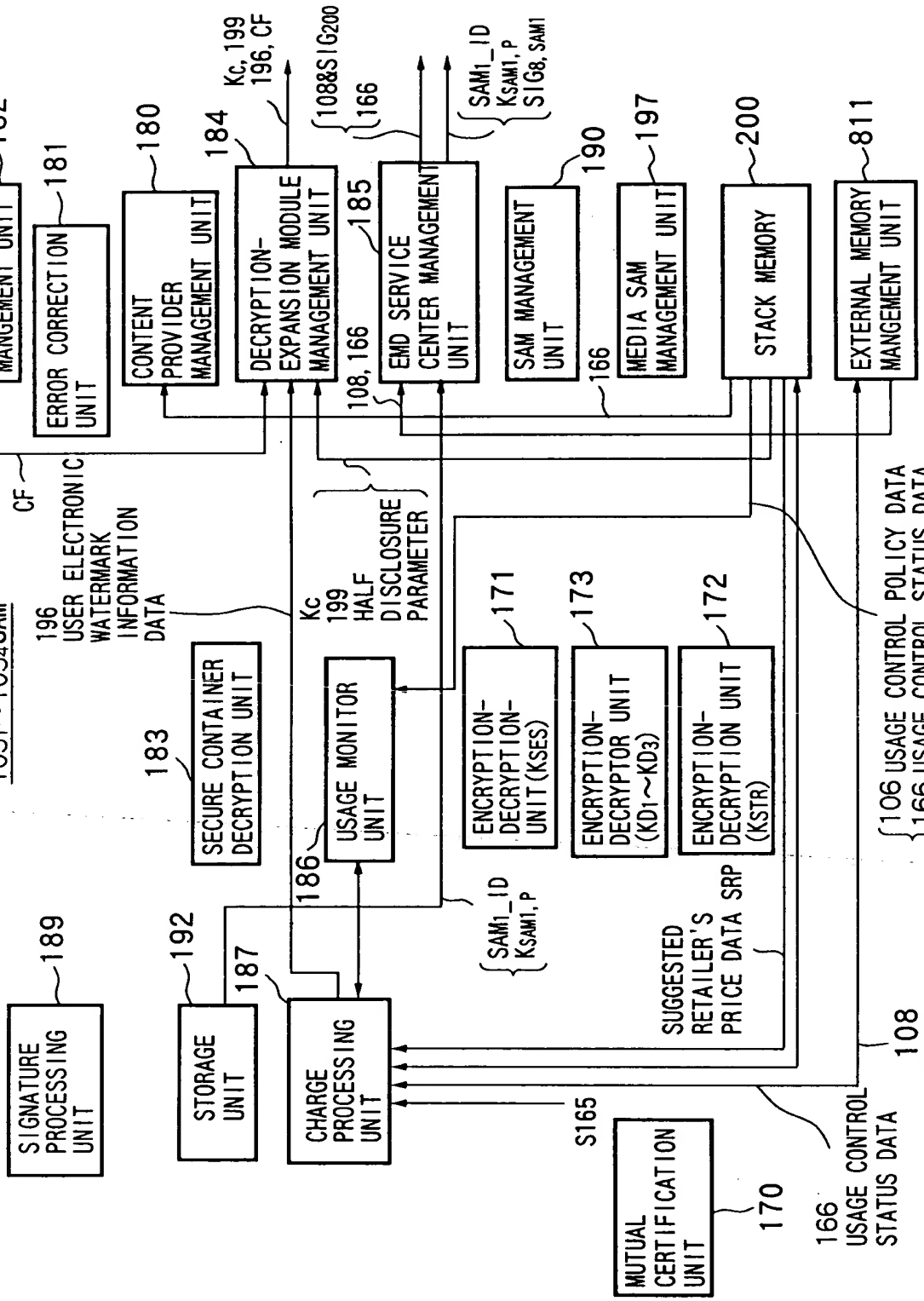

105₁~105₄SAM
DOWNLOAD MEMORY MANGEMENT UNIT
182
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
SAM MANAGEMENT UNIT
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANGEMENT UNIT
811
Kc, 199 196, CF
108&SIG200
166
SAM1_ID KSAM1, P SIG8, SAM1
108, 166
166
CF
196 USER ELECTRONIC WATERMARK INFORMATION DATA
Kc 199 HALF DISCLOSURE PARAMETER
183
SECURE CONTAINER DECRYPTION UNIT
186
USAGE MONITOR UNIT
171
ENCRYPTION-DECRYPTION-UNIT(KSES)
173
ENCRYPTION-DECRYPTOR UNIT (KD1~KD3)
172
ENCRYPTION-DECRYPTION UNIT (KSTR)
106 USAGE CONTROL POLICY DATA
166 USAGE CONTROL STATUS DATA
SAM1_ID KSAM1, P
SUGGESTED RETAILER'S PRICE DATA SRP
189
SIGNATURE PROCESSING UNIT
192
STORAGE UNIT
187
CHARGE PROCESSING UNIT
S165
108 USAGE LOG DATA
MUTUAL CERTIFICATION UNIT
170
166 USAGE CONTROL STATUS DATA

FIG.32

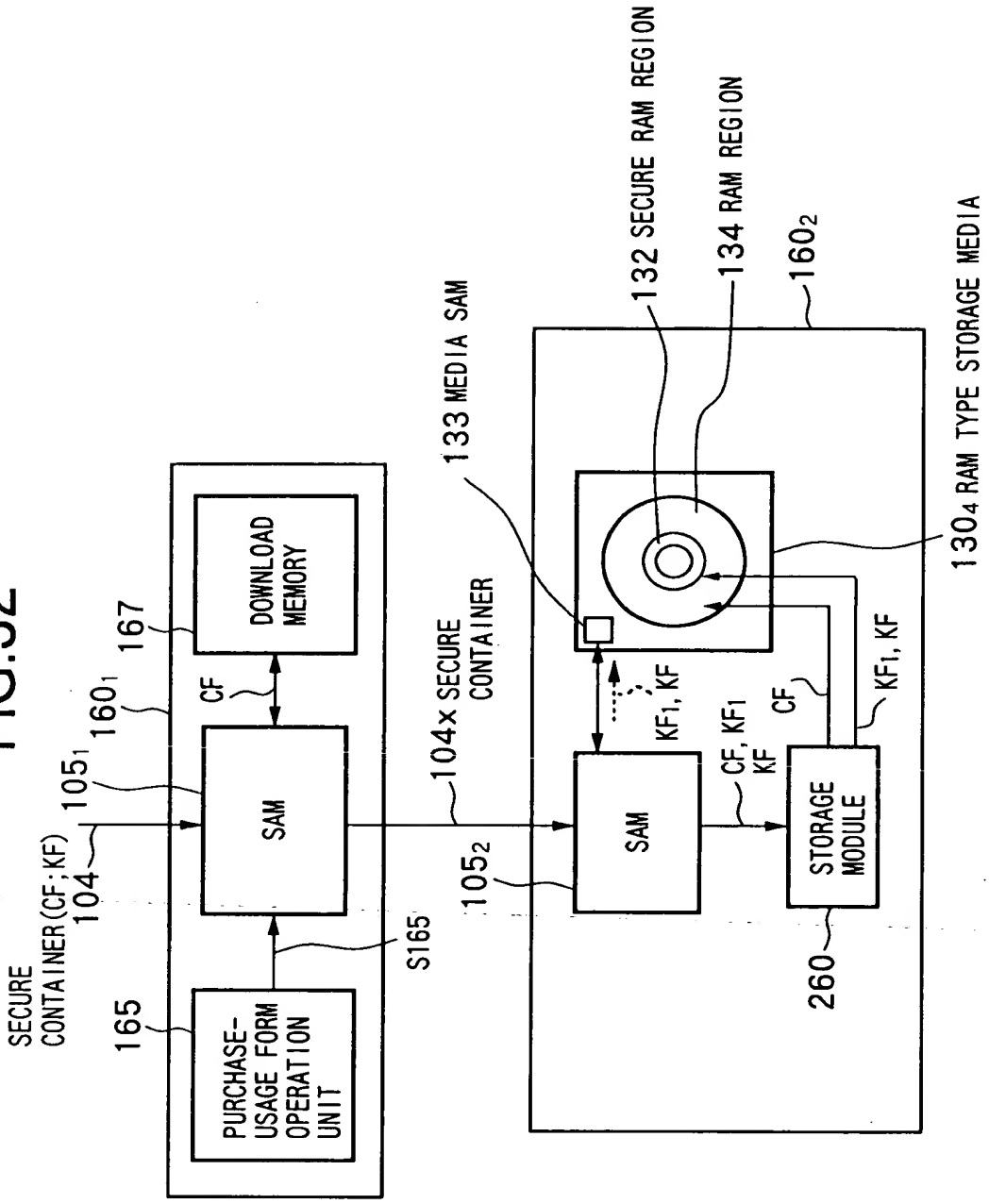
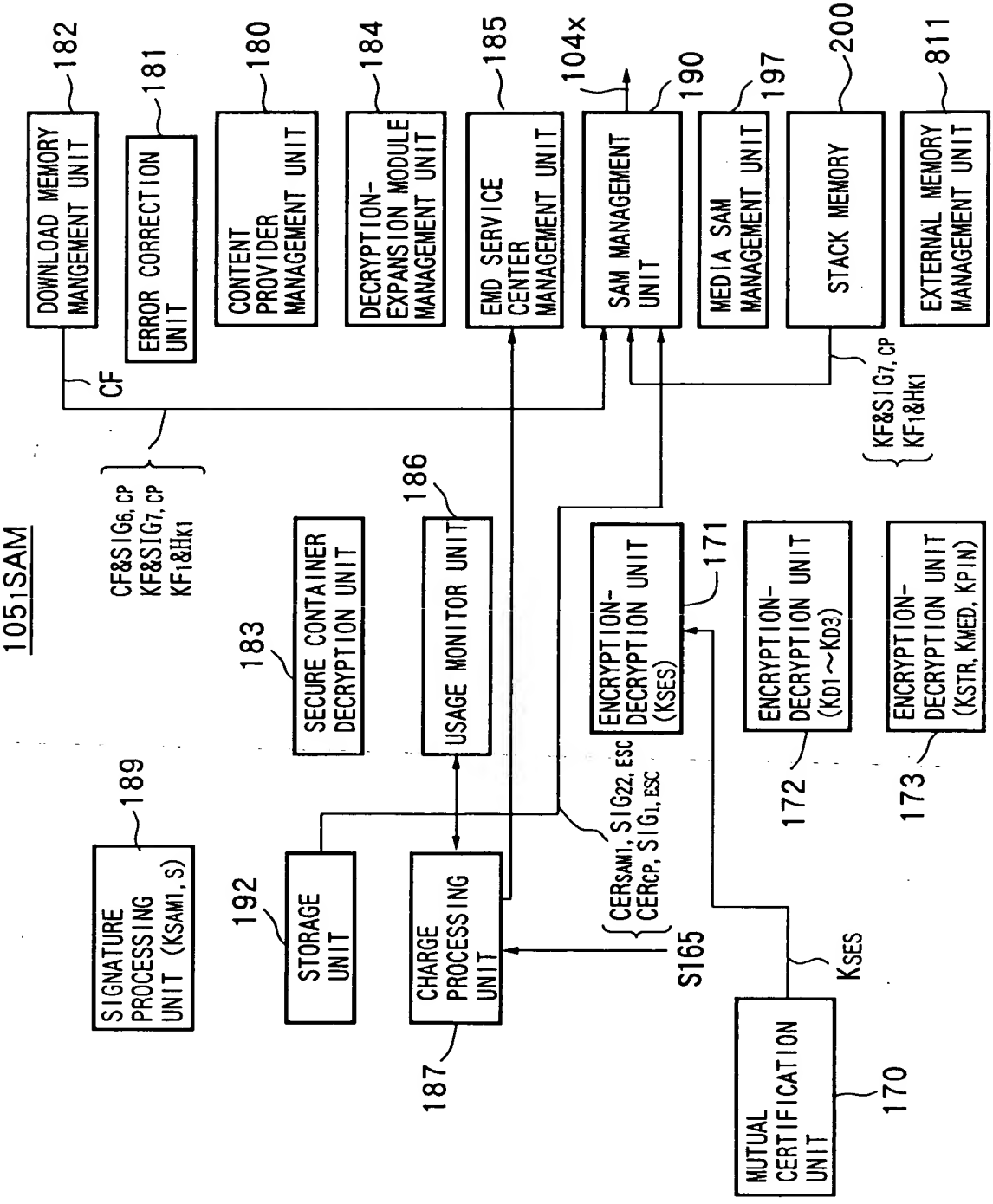

SECURE CONTAINER (CF; KF) 104
165
PURCHASE-USAGE FORM OPERATION UNIT
S165
SAM
105₁
160₁
CF
DOWNLOAD MEMORY
167
104x SECURE CONTAINER
133 MEDIA SAM
105₂
SAM
KF₁, KF
CF, KF₁
KF
CF
KF₁, KF
STORAGE MODULE
260
132 SECURE RAM REGION
134 RAM REGION
160₂
130₄ RAM TYPE STORAGE MEDIA

FIG.33


105₁SAM
DOWNLOAD MEMORY MANGEMENT UNIT
182
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
104x
SAM MANAGEMENT UNIT
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811
CF
CF&SIG6, CP
KF&SIG7, CP
KF1&HK1
KF&SIG7, CP
KF1&HK1
186
USAGE MONITOR UNIT
183
SECURE CONTAINER DECRYPTION UNIT
ENCRYPTION-DECRYPTION UNIT (KSES)
171
ENCRYPTION-DECRYPTION UNIT (KD1~KD3)
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
189
SIGNATURE PROCESSING UNIT (KSAM1, S)
192
STORAGE UNIT
CHARGE PROCESSING UNIT
187
CERSAM1, SIG22, ESC
CERCP, SIG1, ESC
S165
172
173
KSES
MUTUAL CERTIFICATION UNIT
170

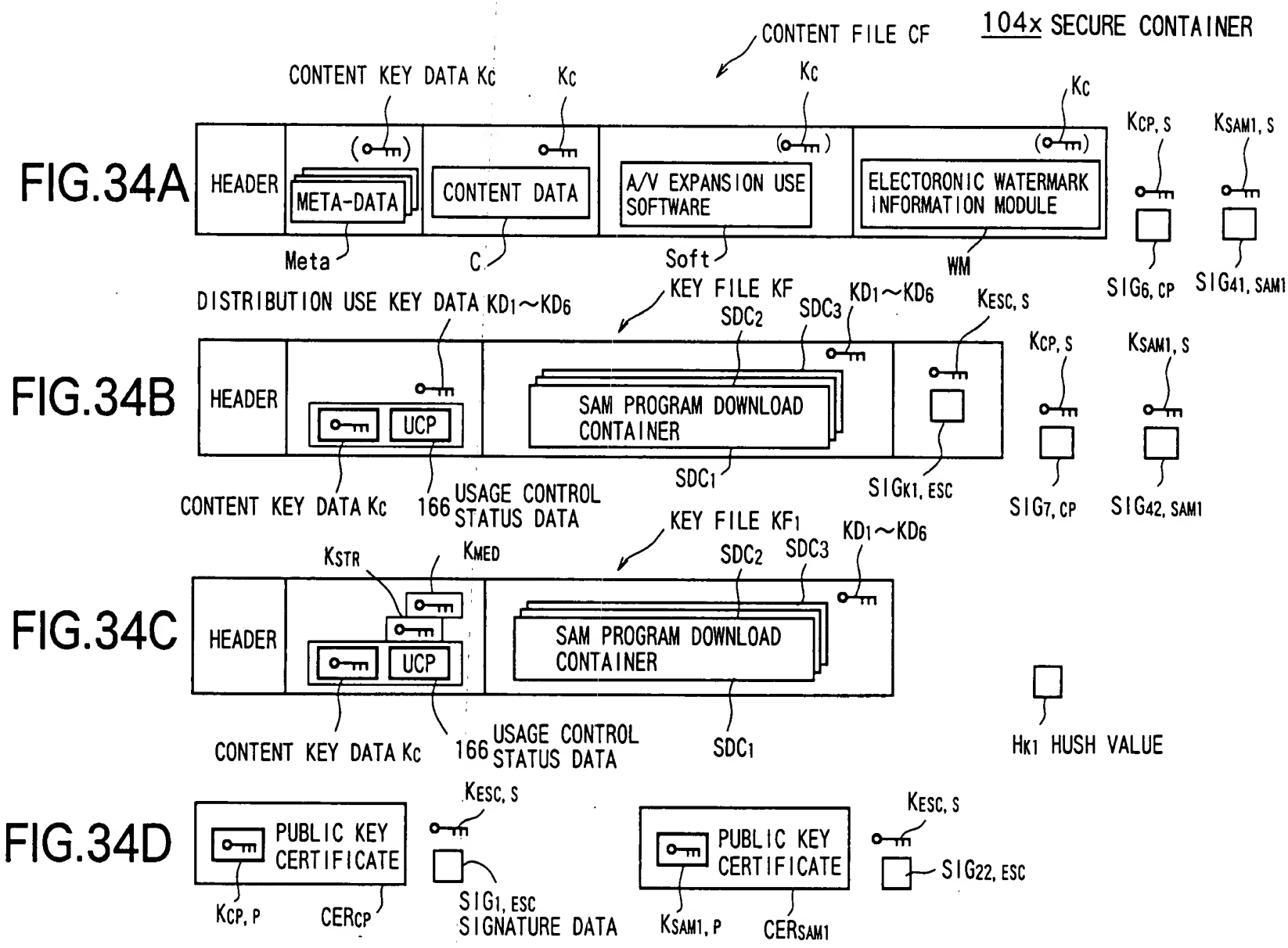


FIG.34A
104x SECURE CONTAINER
CONTENT FILE CF
CONTENT KEY DATA Kc
Kc
Kc
Kc
HEADER
META-DATA
CONTENT DATA
A/V EXPANSION USE SOFTWARE
ELECTORONIC WATERMARK INFORMATION MODULE
KCP, S
KSAM1, S
Meta
C
Soft
WM
SIG6, CP
SIG41, SAM1
FIG.34B
DISTRIBUTION USE KEY DATA KD1~KD6
KEY FILE KF
SDC2
SDC3
KD1~KD6
KESC, S
KCP, S
KSAM1, S
HEADER
UCP
SAM PROGRAM DOWNLOAD CONTAINER
SDC1
SIGK1, ESC
SIG7, CP
SIG42, SAM1
CONTENT KEY DATA Kc
166 USAGE CONTROL STATUS DATA
FIG.34C
KEY FILE KF1
KSTR
KMED
SDC2
SDC3
KD1~KD6
HEADER
UCP
SAM PROGRAM DOWNLOAD CONTAINER
CONTENT KEY DATA Kc
166 USAGE CONTROL STATUS DATA
SDC1
HK1 HUSH VALUE
FIG.34D
KESC, S
PUBLIC KEY CERTIFICATE
KCP, P
CERCP
SIG1, ESC SIGNATURE DATA
PUBLIC KEY CERTIFICATE
KESC, S
SIG22, ESC
KSAM1, P
CERSAM1

FIG.35

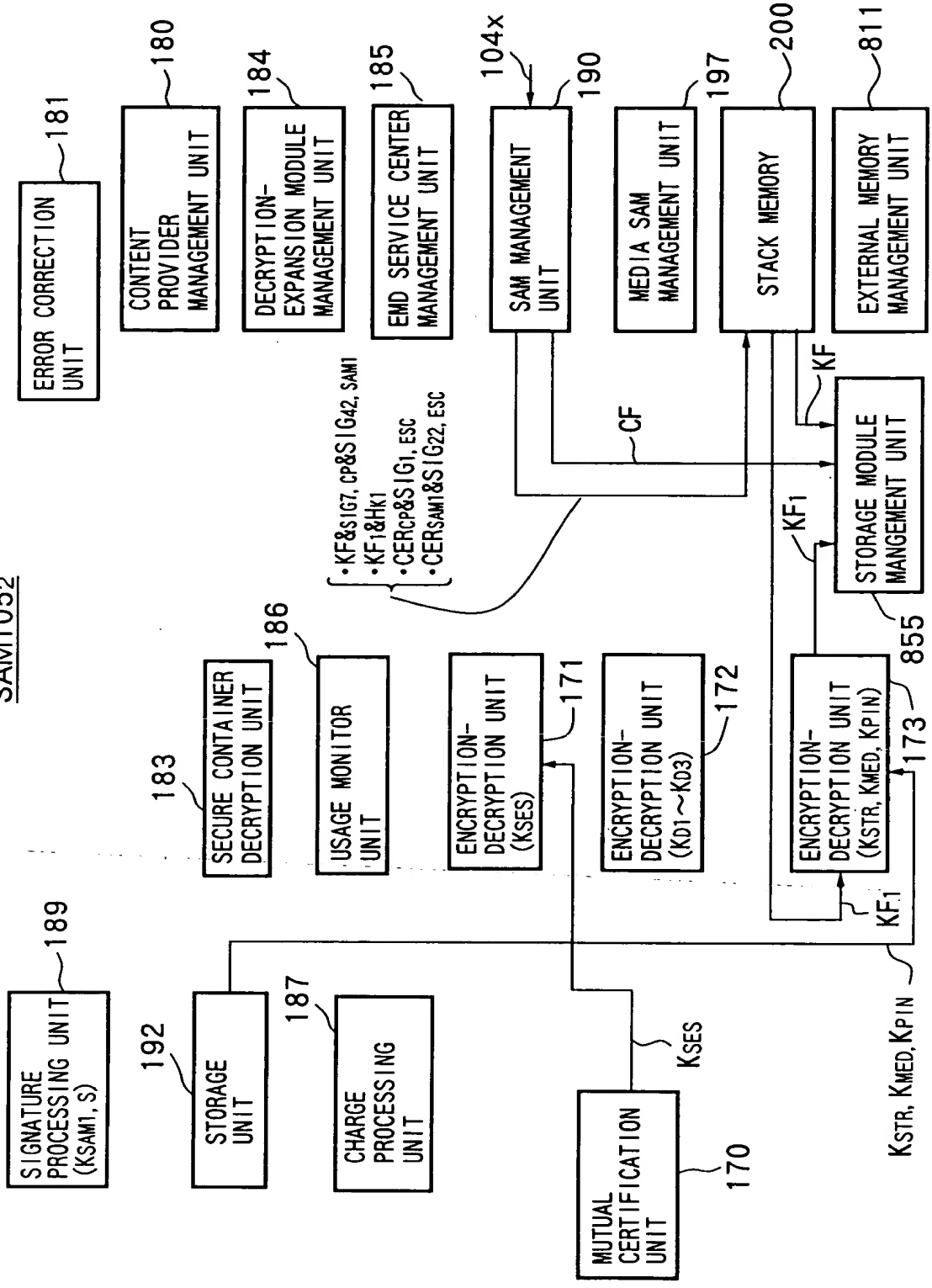

SAM1052
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
SAM MANAGEMENT UNIT
104x
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811
•KF&SIG7, CP&SIG42, SAM1
•KF1&HK1
•CERCP&SIG1, ESC
•CERSAM1&SIG22, ESC
CF
KF
KF1
STORAGE MODULE MANGEMENT UNIT
855
SECURE CONTAINER DECRYPTION UNIT
183
USAGE MONITOR UNIT
186
ENCRYPTION-DECRYPTION UNIT (KSES)
171
ENCRYPTION-DECRYPTION UNIT (KD1~KD3)
172
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
173
KF1
SIGNATURE PROCESSING UNIT (KSAM1, S)
189
STORAGE UNIT
192
CHARGE PROCESSING UNIT
187
KSES
MUTUAL CERTIFICATION UNIT
170
KSTR, KMED, KPIN

FIG.36

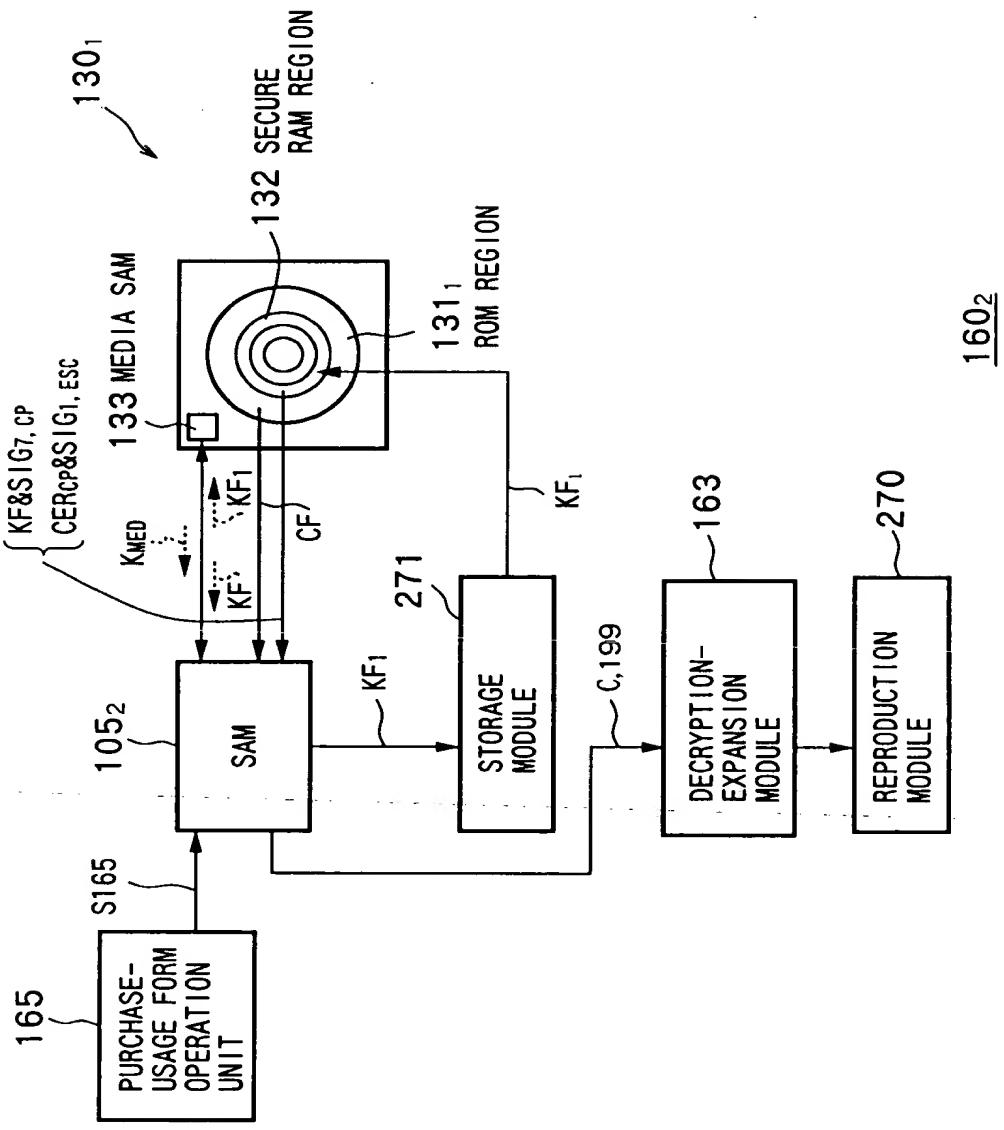

130_1
132 SECURE RAM REGION
133 MEDIA SAM
131_1 ROM REGION
160_2
KF&SIG7, CP
CERCP&SIG1, ESC
K_{MED}
KF
KF_1
CF
KF_1
105_2
SAM
KF_1
271
STORAGE MODULE
C, 199
163
DECRYPTION-EXPANSION MODULE
270
REPRODUCTION MODULE
S165
165
PURCHASE-USAGE FORM OPERATION UNIT

FIG.37

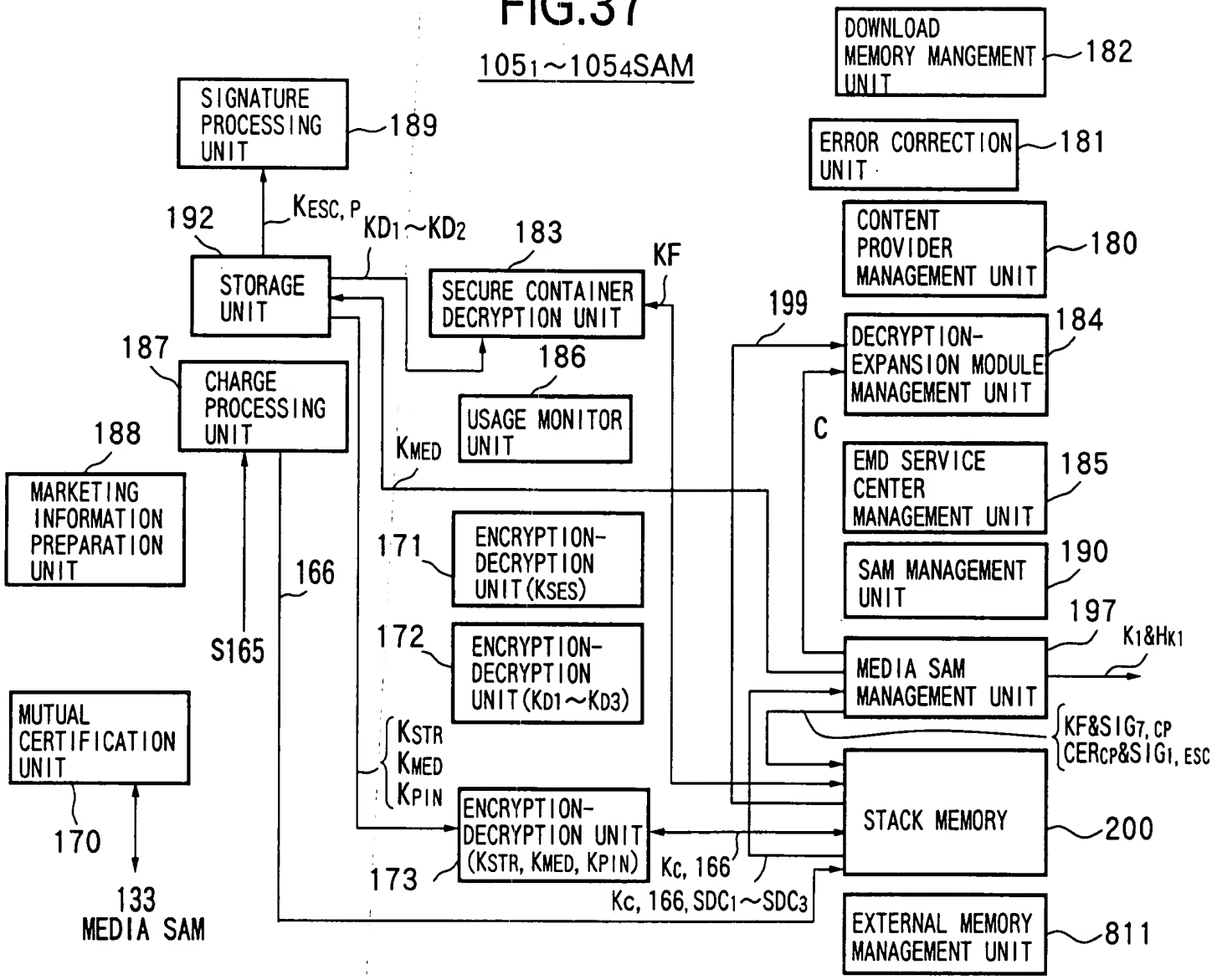

1051~1054SAM
SIGNATURE PROCESSING UNIT
189
KESC, P
192
STORAGE UNIT
KD1~KD2
183
SECURE CONTAINER DECRYPTION UNIT
KF
186
USAGE MONITOR UNIT
187
CHARGE PROCESSING UNIT
188
MARKETING INFORMATION PREPARATION UNIT
KMED
166
S165
171
ENCRYPTION-DECRYPTION UNIT(KSES)
172
ENCRYPTION-DECRYPTION UNIT(KD1~KD3)
KSTR
KMED
KPIN
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
173
MUTUAL CERTIFICATION UNIT
170
133
MEDIA SAM
Kc, 166
Kc, 166, SDC1~SDC3
DOWNLOAD MEMORY MANGEMENT UNIT
182
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
199
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
C
EMD SERVICE CENTER MANAGEMENT UNIT
185
SAM MANAGEMENT UNIT
190
197
K1&HK1
MEDIA SAM MANAGEMENT UNIT
KF&SIG7, CP
CERCP&SIG1, ESC
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811

FIG.38

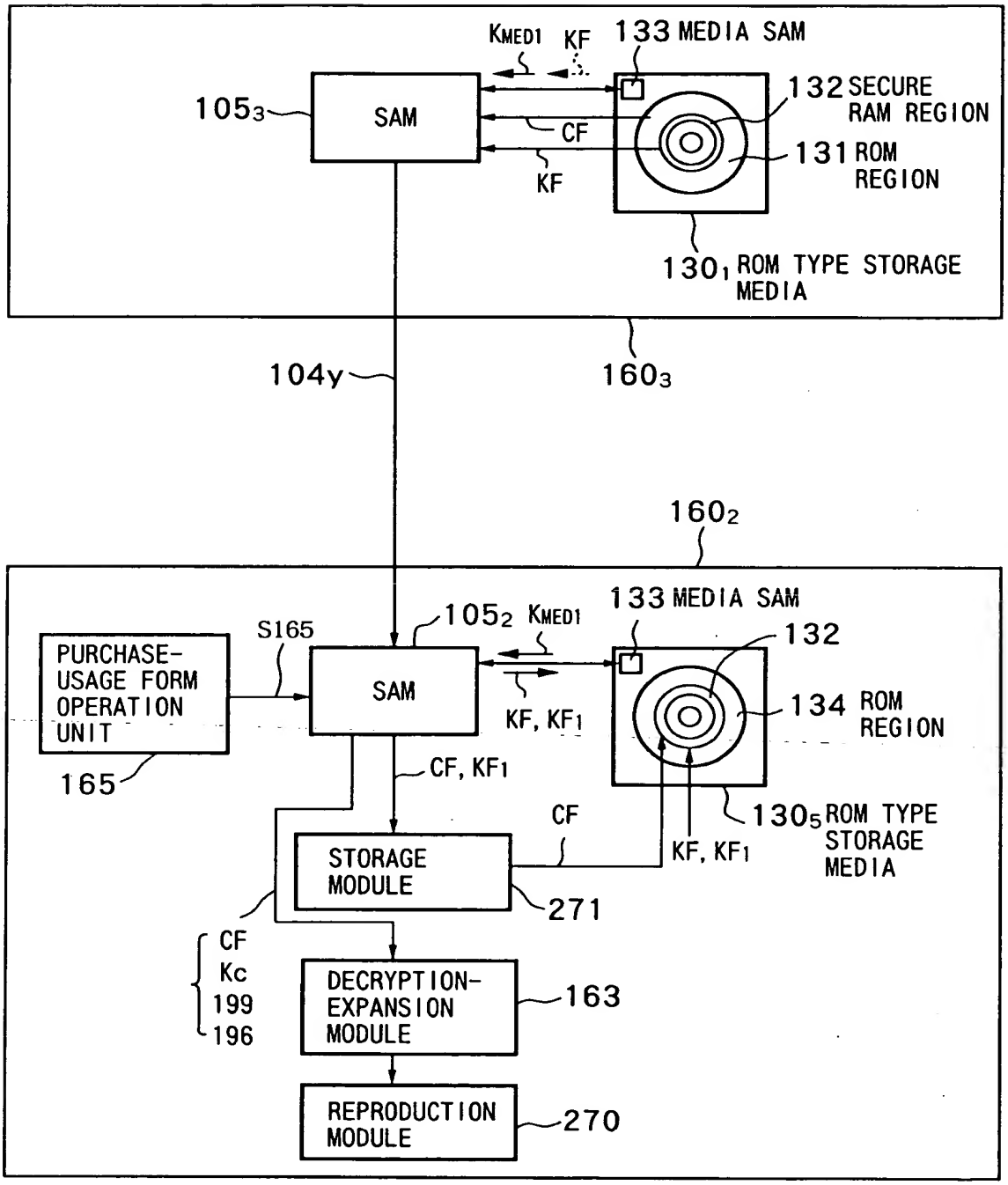

KMED1
KF
133 MEDIA SAM
105₃
SAM
CF
KF
132 SECURE RAM REGION
131 ROM REGION
130₁ ROM TYPE STORAGE MEDIA
160₃
104y
160₂
105₂ KMED1
133 MEDIA SAM
S165
PURCHASE-USAGE FORM OPERATION UNIT
165
SAM
KF, KF1
132
134 ROM REGION
CF, KF1
CF
KF, KF1
130₅ ROM TYPE STORAGE MEDIA
STORAGE MODULE
271
CF
Kc
199
196
DECRYPTION-EXPANSION MODULE
163
REPRODUCTION MODULE
270

FIG.39

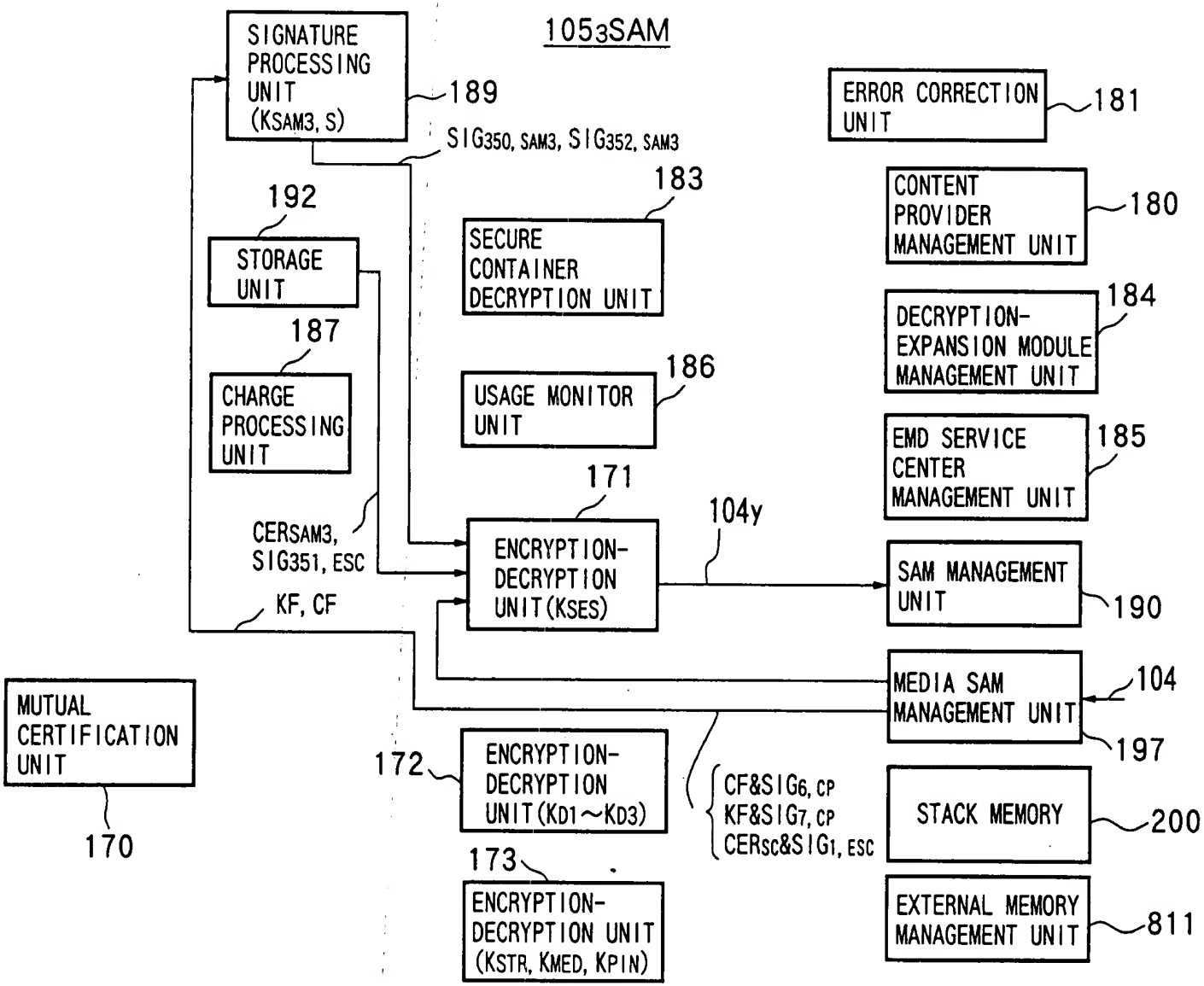


FIG.40A

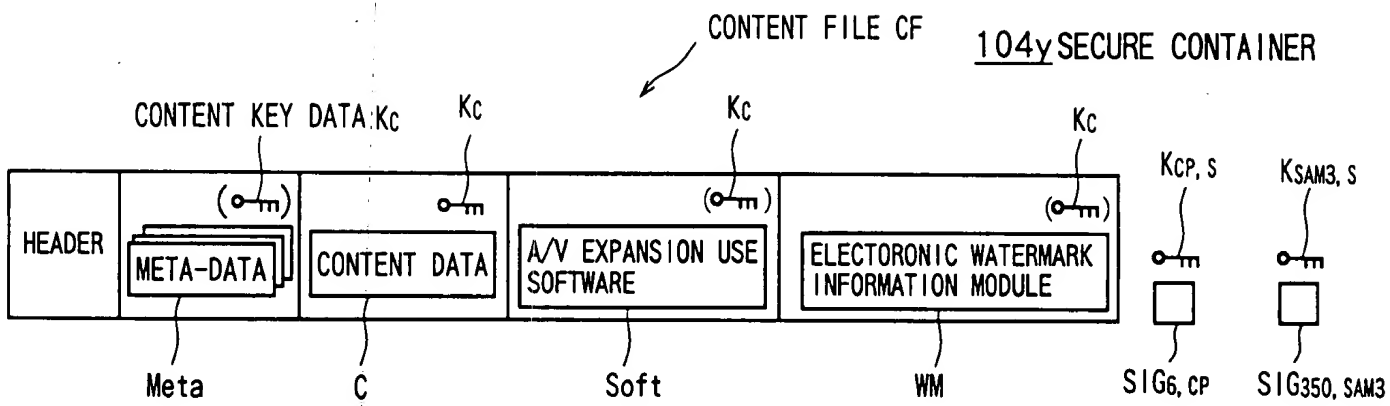


FIG.40B

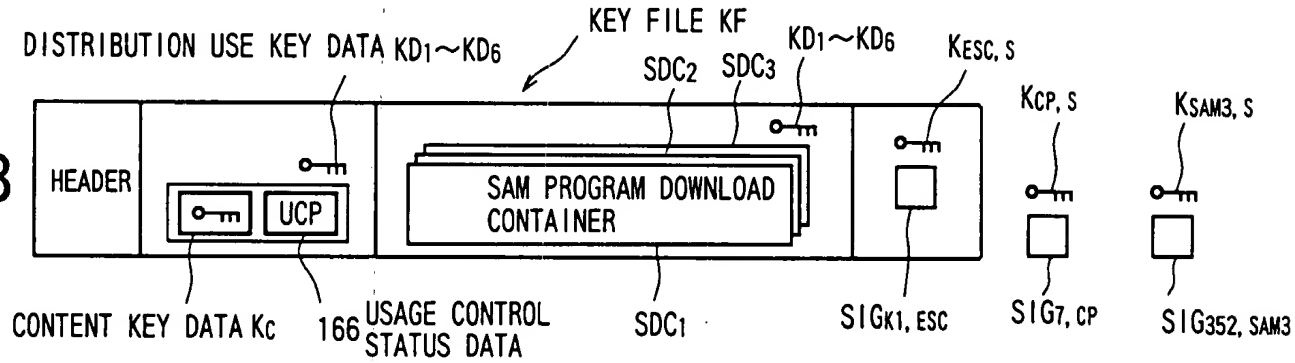


FIG.40C

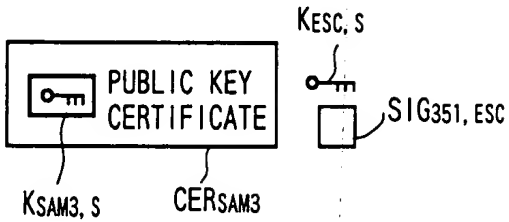


FIG.41

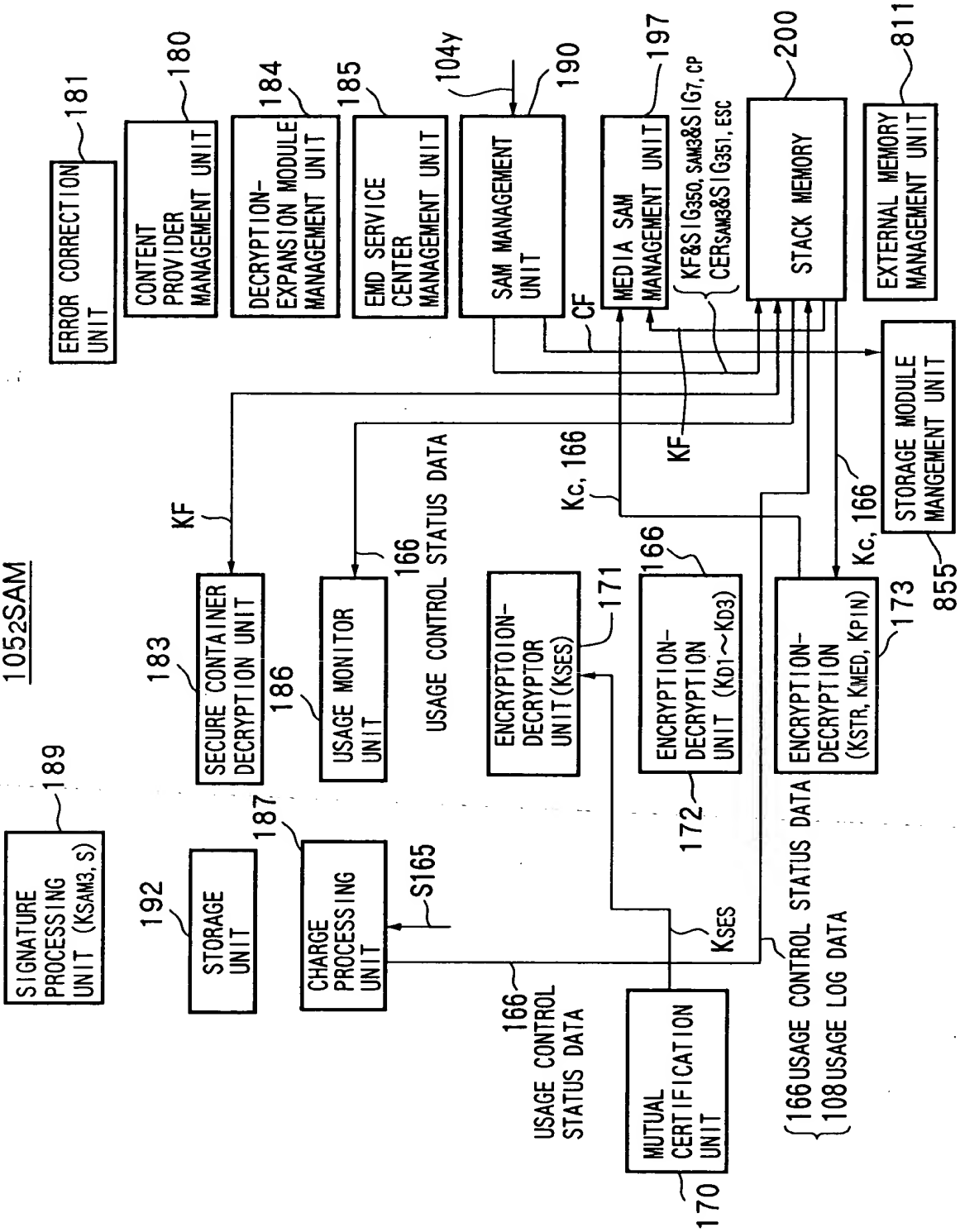

105₂SAM
ERROR CORRECTION UNIT
181
CONTENT PROVIDER MANAGEMENT UNIT
180
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
104y
SAM MANAGEMENT UNIT
190
CF
MEDIA SAM MANAGEMENT UNIT
197
KF&SIG350, SAM3&SIG7, CP
CERSAM3&SIG351, ESC
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811
STORAGE MODULE MANGEMENT UNIT
855
KF
Kc, 166
SECURE CONTAINER DECRYPTION UNIT
183
USAGE MONITOR UNIT
186
166
USAGE CONTROL STATUS DATA
ENCRYPTOION-DECRYPTOR UNIT(KSES)
171
ENCRYPTION-DECRYPTION UNIT (KD1~KD3)
166
172
ENCRYPTION-DECRYPTION (KSTR, KMED, KPIN)
173
SIGNATURE PROCESSING UNIT (KSAM3, S)
189
STORAGE UNIT
192
CHARGE PROCESSING UNIT
187
S165
KSES
MUTUAL CERTIFICATION UNIT
170
166 USAGE CONTROL STATUS DATA
108 USAGE LOG DATA

FIG.42A 101(CP)→SAM105$_1$ (IN-BAND)

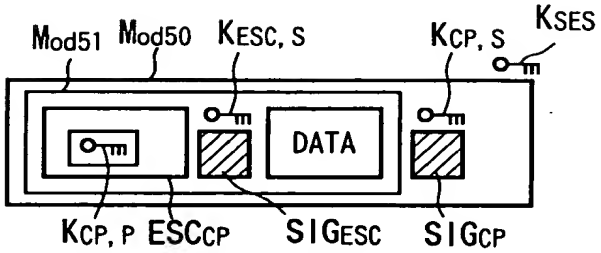


FIG.42B 101(CP)→SAM105$_1$ (OUT-OF-BAND)

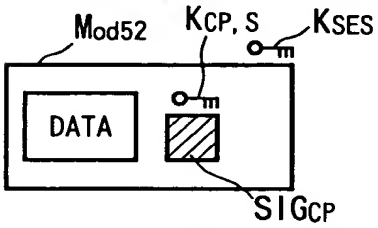


FIG.42C 102(ESC)→SAM105$_1$ (OUT-OF-BAND)

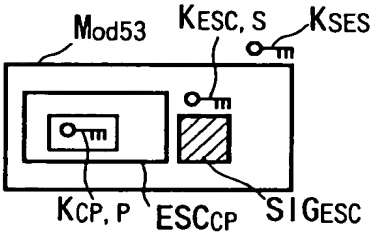


FIG.42D SAM105$_1$→101(CP) (IN-BAND)

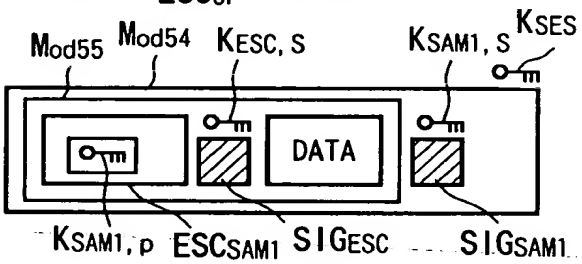


FIG.42E SAM105$_1$→101(CP) (OUT-OF-BAND)

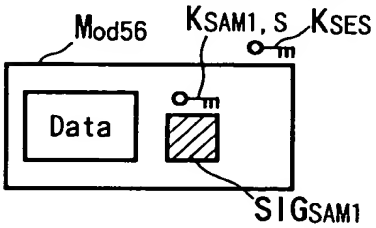


FIG.42F 102(ESC)→101(CP) (OUT-OF-BAND)

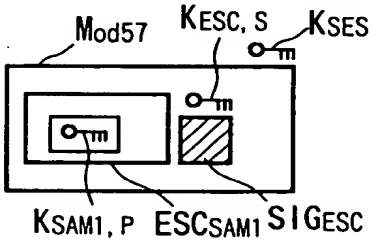


FIG.43G 101(CP)→102(ESC) (IN-BAND)

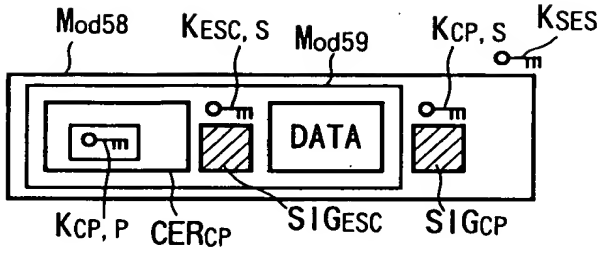


FIG.43H 101(CP)→102(ESC) (OUT-OF- BAND)

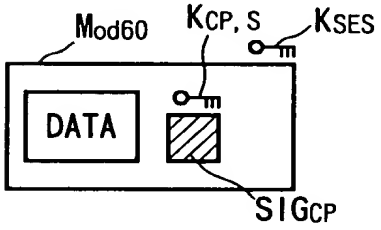


FIG.43I SAM1051→102(ESC) (IN-BAND)

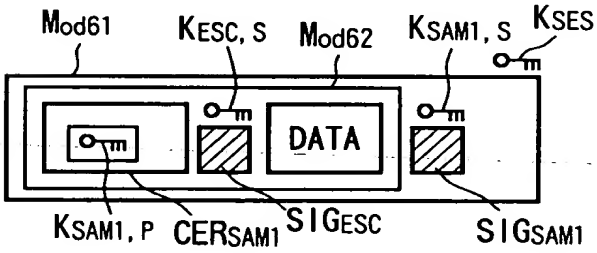


FIG.43J SAM1051→102(ESC) (OUT-OF-BAND)

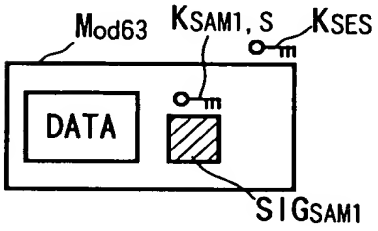


FIG.44

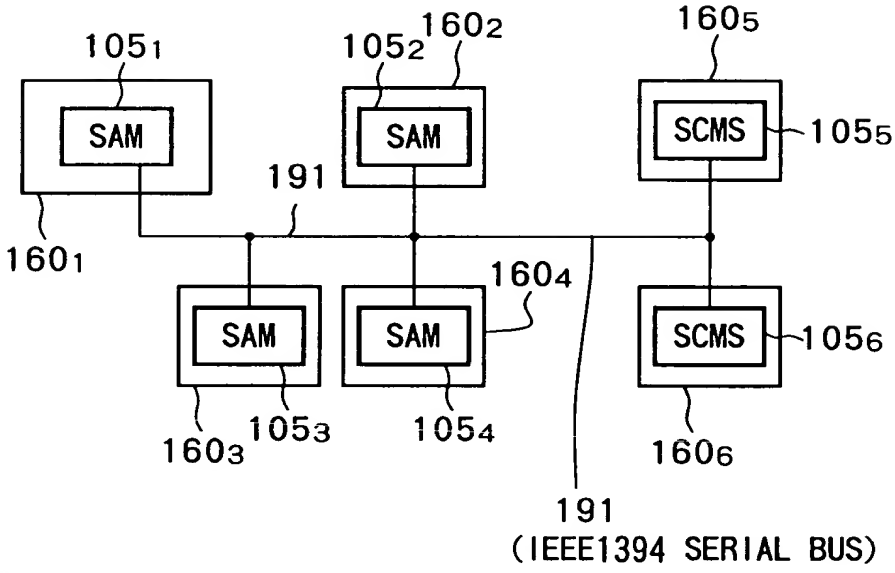

1051
1052
1602
1605
SAM
SAM
SCMS
1055
191
1601
1604
SAM
SAM
SCMS
1056
1603
1053
1054
1606
191
(IEEE1394 SERIAL BUS)

FIG.45

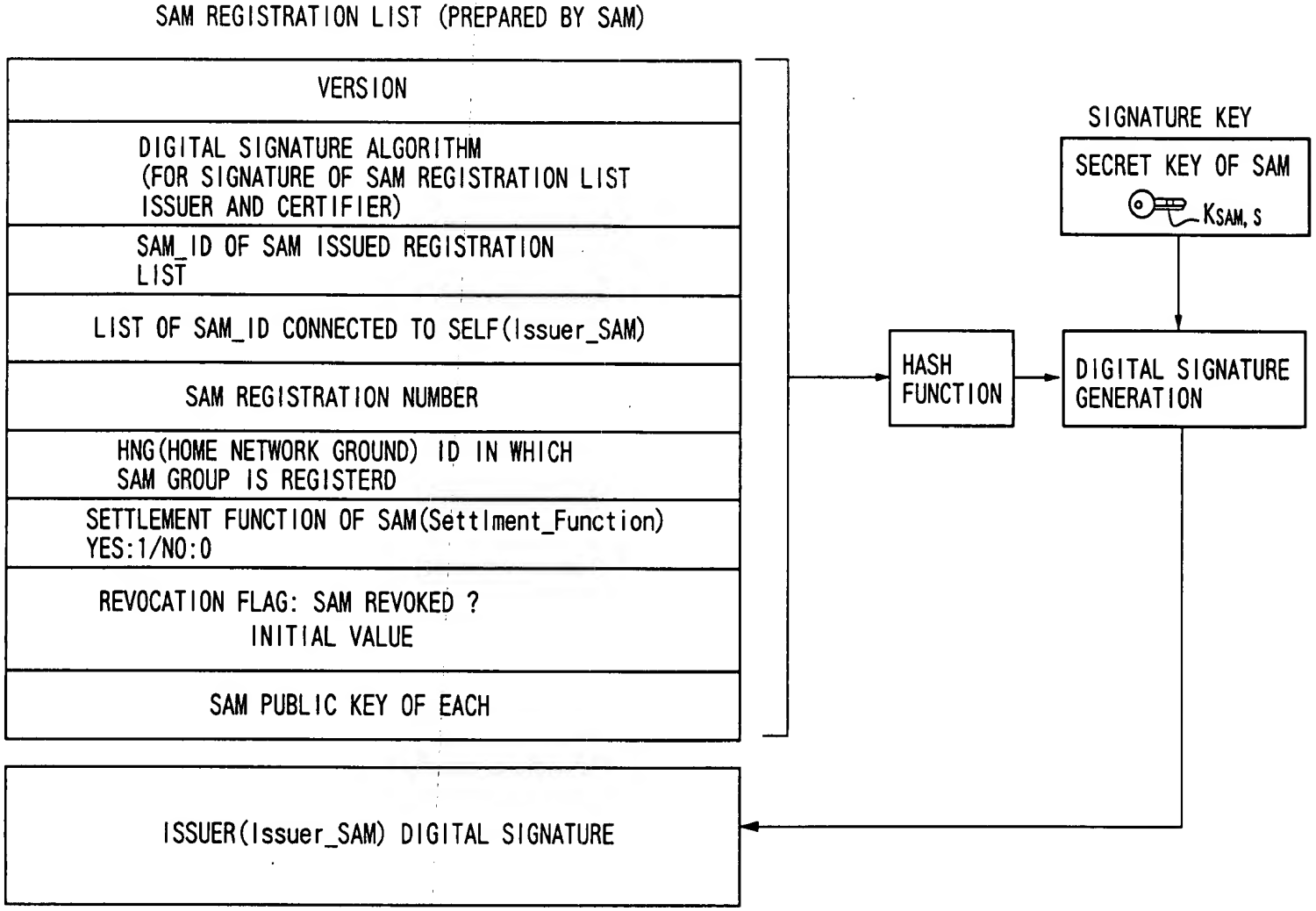


FIG.46

SAM REGISTRATION LIST (PREPARED BY EMD SERVICE CENTER)

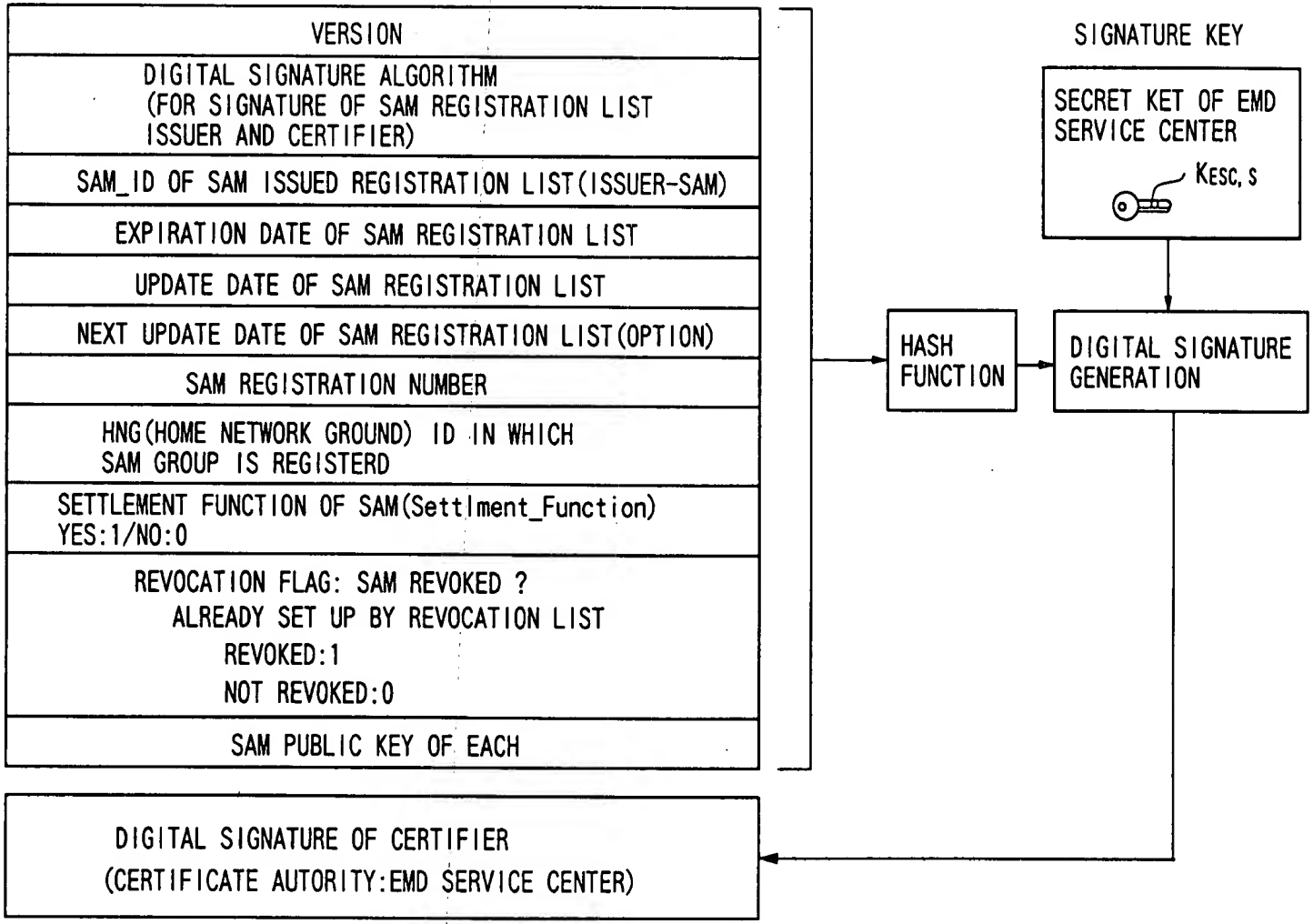


FIG.47

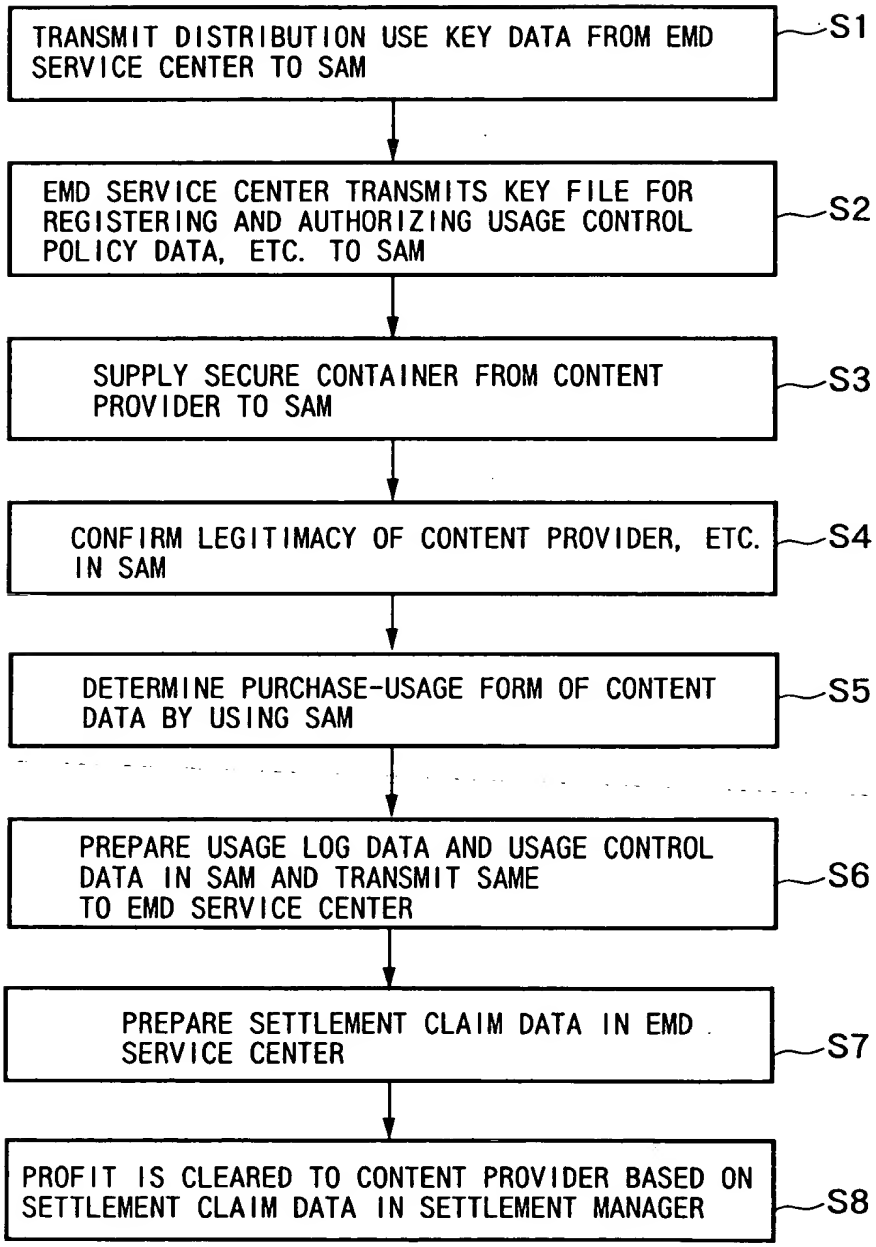

TRANSMIT DISTRIBUTION USE KEY DATA FROM EMD SERVICE CENTER TO SAM
S1
EMD SERVICE CENTER TRANSMITS KEY FILE FOR REGISTERING AND AUTHORIZING USAGE CONTROL POLICY DATA, ETC. TO SAM
S2
SUPPLY SECURE CONTAINER FROM CONTENT PROVIDER TO SAM
S3
CONFIRM LEGITIMACY OF CONTENT PROVIDER, ETC. IN SAM
S4
DETERMINE PURCHASE-USAGE FORM OF CONTENT DATA BY USING SAM
S5
PREPARE USAGE LOG DATA AND USAGE CONTROL DATA IN SAM AND TRANSMIT SAME TO EMD SERVICE CENTER
S6
PREPARE SETTLEMENT CLAIM DATA IN EMD SERVICE CENTER
S7
PROFIT IS CLEARED TO CONTENT PROVIDER BASED ON SETTLEMENT CLAIM DATA IN SETTLEMENT MANAGER
S8

FIG.48

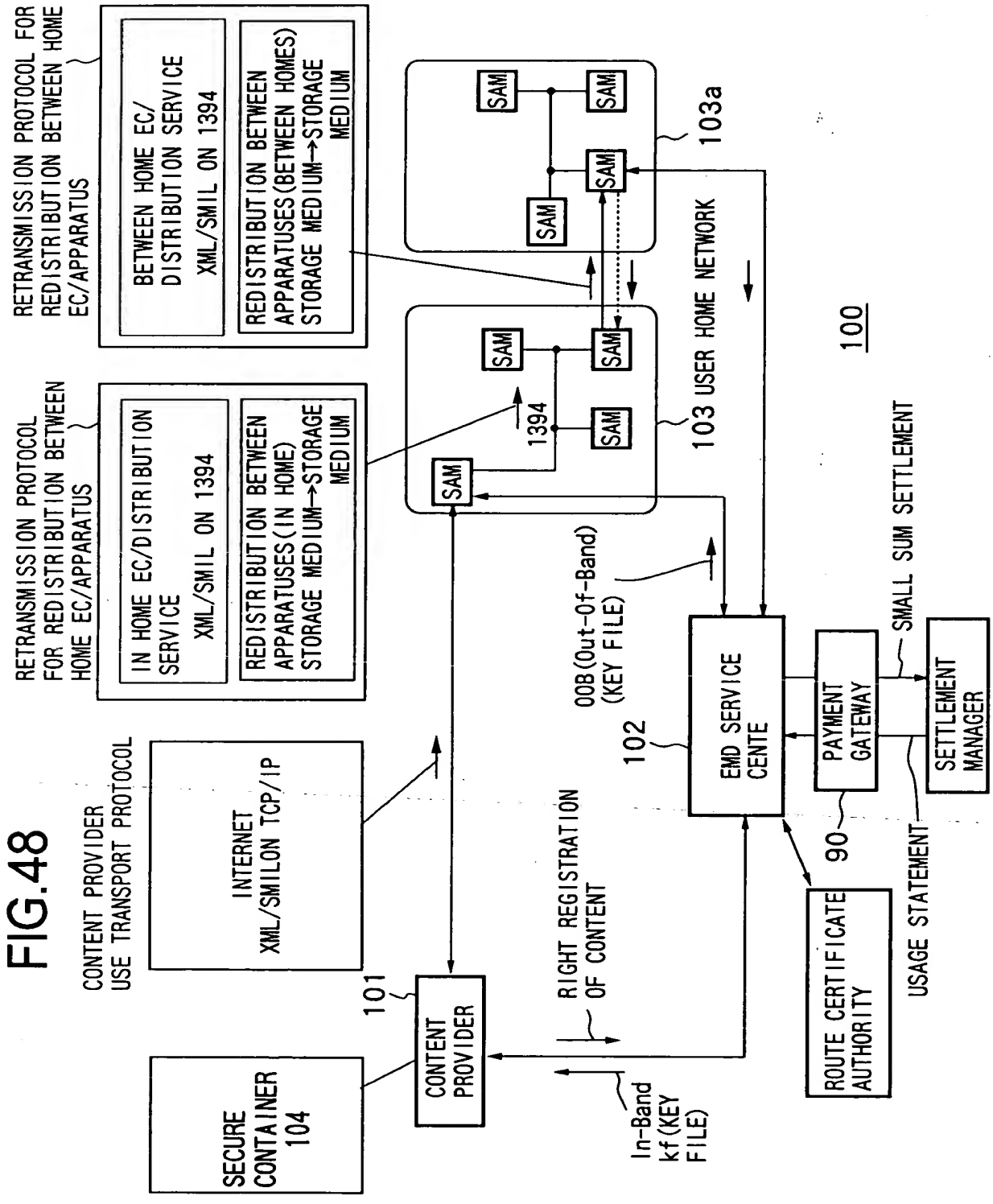

CONTENT PROVIDER USE TRANSPORT PROTOCOL
INTERNET XML/SMILON TCP/IP
SECURE CONTAINER 104
CONTENT PROVIDER
101
RIGHT REGISTRATION OF CONTENT
In-Band kf(KEY FILE)
RETRANSMISSION PROTOCOL FOR REDISTRIBUTION BETWEEN HOME EC/APPARATUS
IN HOME EC/DISTRIBUTION SERVICE XML/SMIL ON 1394
REDISTRIBUTION BETWEEN APPARATUSES(IN HOME) STORAGE MEDIUM→STORAGE MEDIUM
RETRANSMISSION PROTOCOL FOR REDISTRIBUTION BETWEEN HOME EC/APPARATUS
BETWEEN HOME EC/ DISTRIBUTION SERVICE XML/SMIL ON 1394
REDISTRIBUTION BETWEEN APPARATUSES(BETWEEN HOMES) STORAGE MEDIUM→STORAGE MEDIUM
1394
SAM
103 USER HOME NETWORK
103a
100
OOB(Out-Of-Band) (KEY FILE)
102
EMD SERVICE CENTE
PAYMENT GATEWAY
SETTLEMENT MANAGER
SMALL SUM SETTLEMENT
90
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY

FIG.49

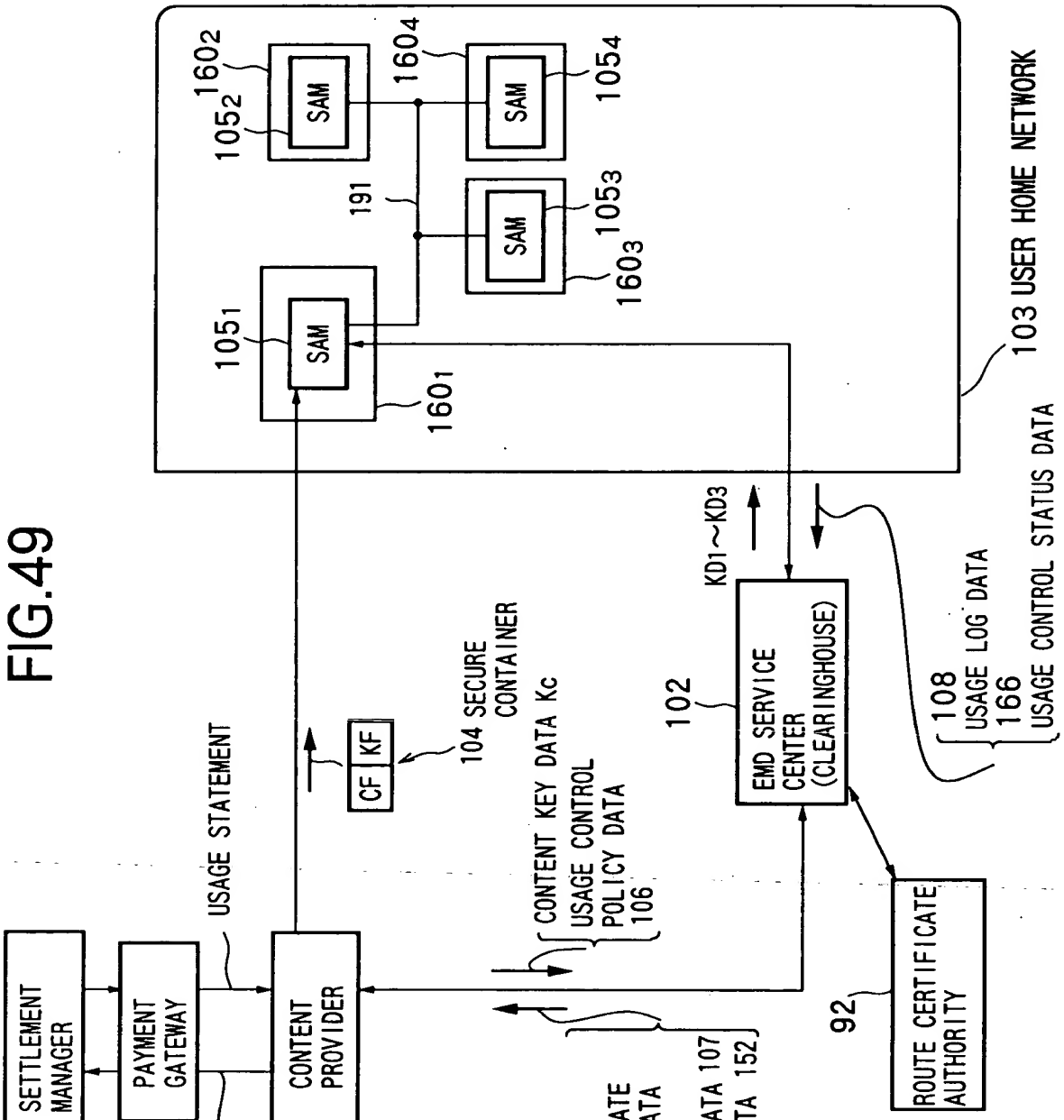

SETTLEMENT MANAGER
PAYMENT GATEWAY
CONTENT PROVIDER
ROUTE CERTIFICATE AUTHORITY
EMD SERVICE CENTER (CLEARINGHOUSE)
SAM
CF
KF
91
90
101
92
102
152
191
104 SECURE CONTAINER
103 USER HOME NETWORK
USAGE STATEMENT
SETTLEMENT CLAIM DATA
CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA 106
KD1~KD3
108 USAGE LOG DATA
166 USAGE CONTROL STATUS DATA
•KEY FILE KF
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 107
•SETTLEMENT CLAIM DATA 152

FIG.50

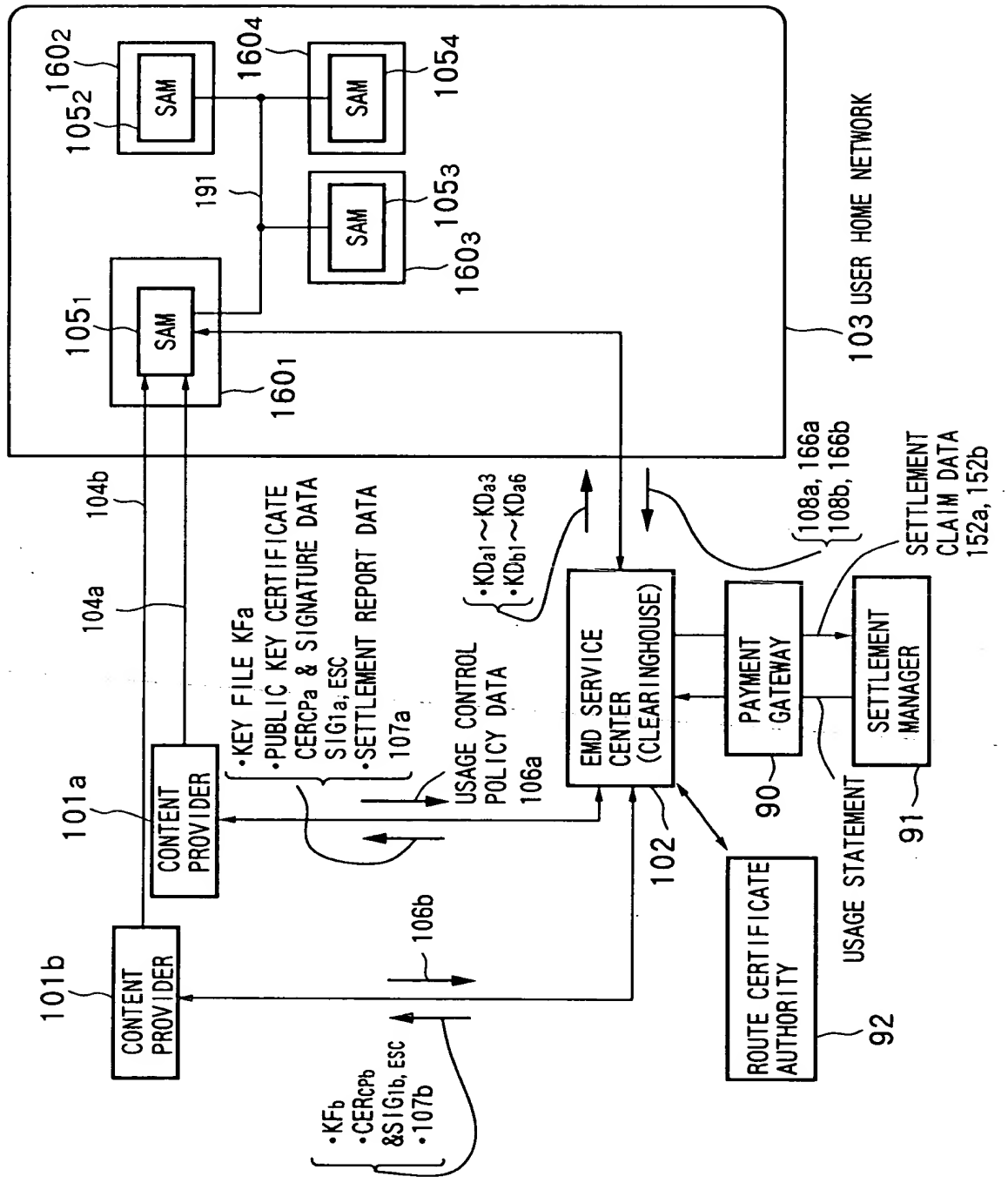

SAM
SAM
SAM
SAM
160_2
160_4
160_3
160_1
105_2
105_4
105_3
105_1
191
103 USER HOME NETWORK
104b
104a
101a
CONTENT PROVIDER
101b
CONTENT PROVIDER
•KEY FILE KFa
•PUBLIC KEY CERTIFICATE CERCPa & SIGNATURE DATA SIG1a, ESC
•SETTLEMENT REPORT DATA 107a
USAGE CONTROL POLICY DATA 106a
106b
•KFb
•CERCPb &SIG1b, ESC
•107b
•KDa1~KDa3
•KDb1~KDa6
EMD SERVICE CENTER (CLEARINGHOUSE)
102
108a, 166a
108b, 166b
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
SETTLEMENT CLAIM DATA 152a, 152b
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY
92

FIG.51

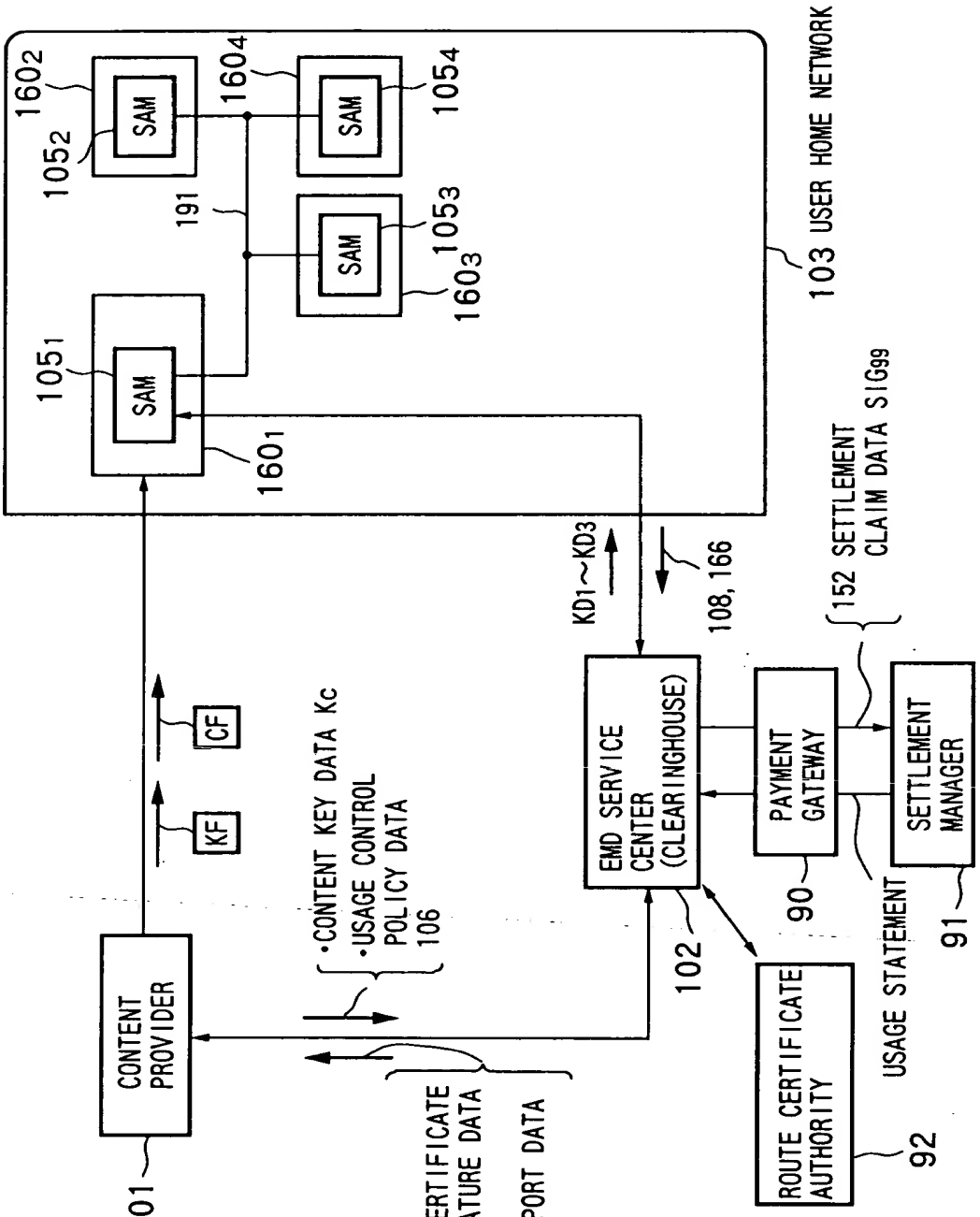

103 USER HOME NETWORK
SAM
1051
1052
1053
1054
1601
1602
1603
1604
191
CONTENT PROVIDER
101
KF
CF
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
•KEY FILE KF
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
••SETTLEMENT REPORT DATA
107
EMD SERVICE CENTER (CLEARINGHOUSE)
102
KD1~KD3
108, 166
PAYMENT GATEWAY
90
152 SETTLEMENT CLAIM DATA SIG99
SETTLEMENT MANAGER
91
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY
92

FIG.52

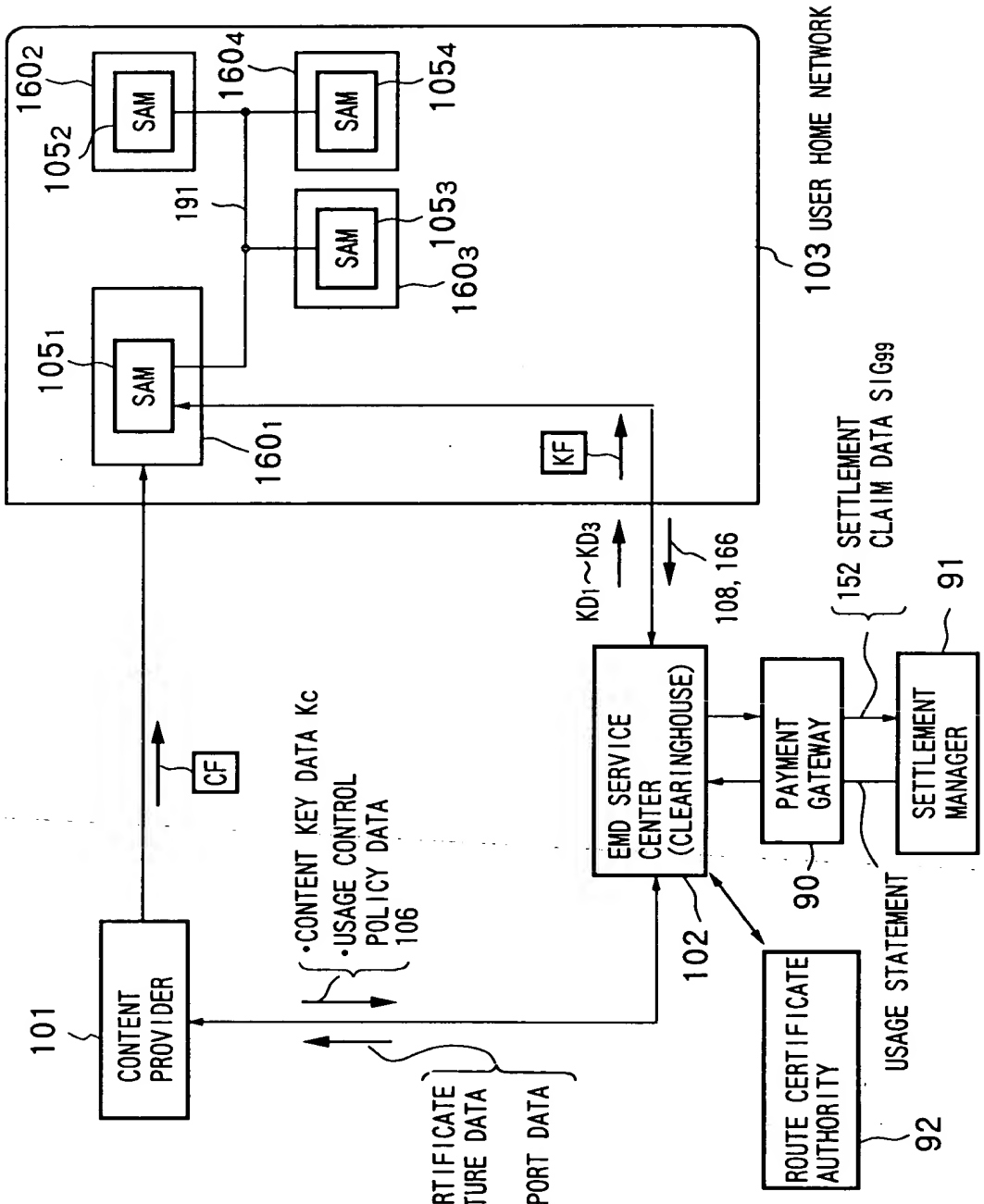


FIG.53

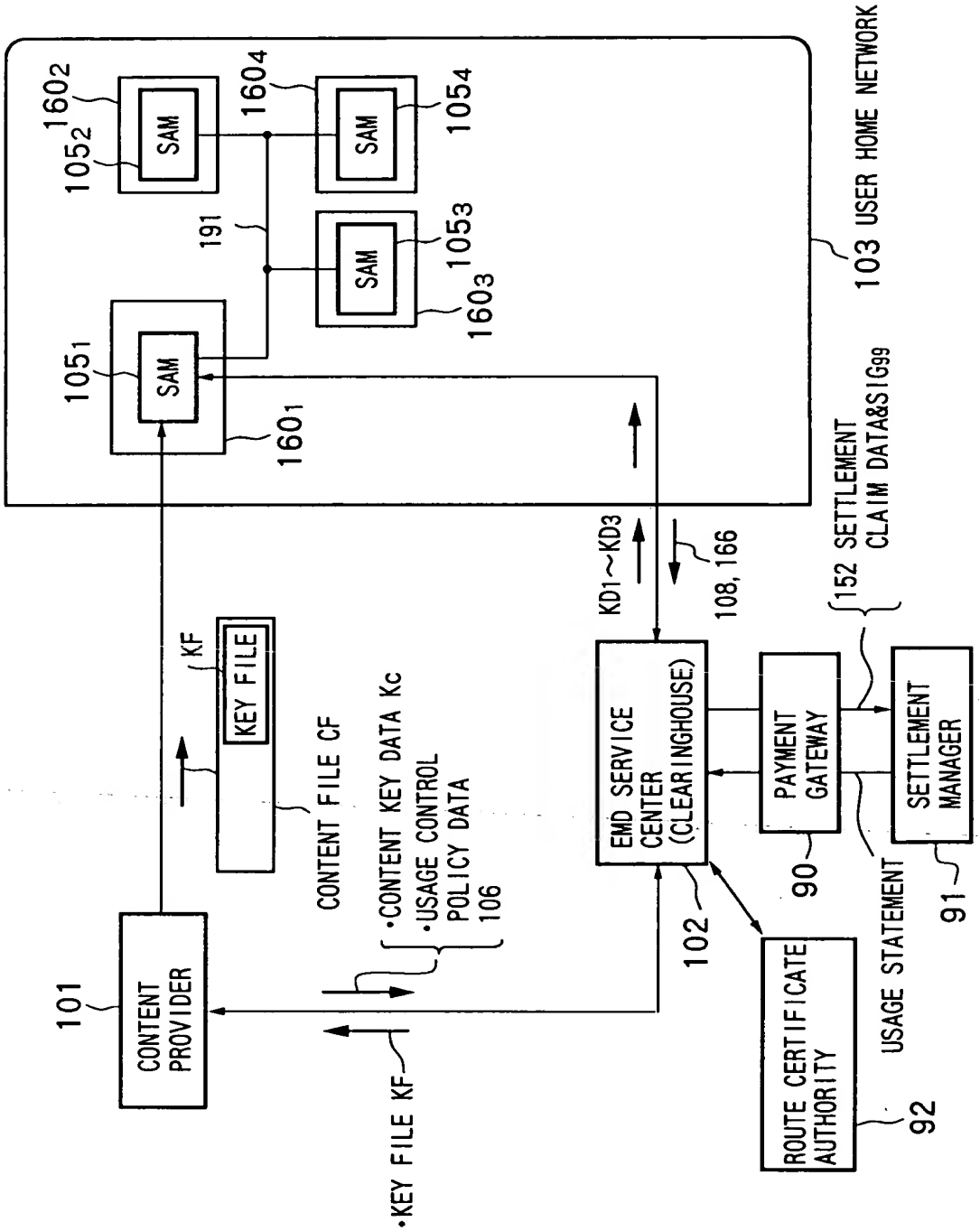

103 USER HOME NETWORK
SAM
1052
1602
1604
1054
1053
1603
191
1051
1601
152 SETTLEMENT CLAIM DATA&SIG99
KD1~KD3
108, 166
KF
KEY FILE
CONTENT FILE CF
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
101
CONTENT PROVIDER
102
90
91
•KEY FILE KF
ROUTE CERTIFICATE AUTHORITY
USAGE STATEMENT
92

FIG.54

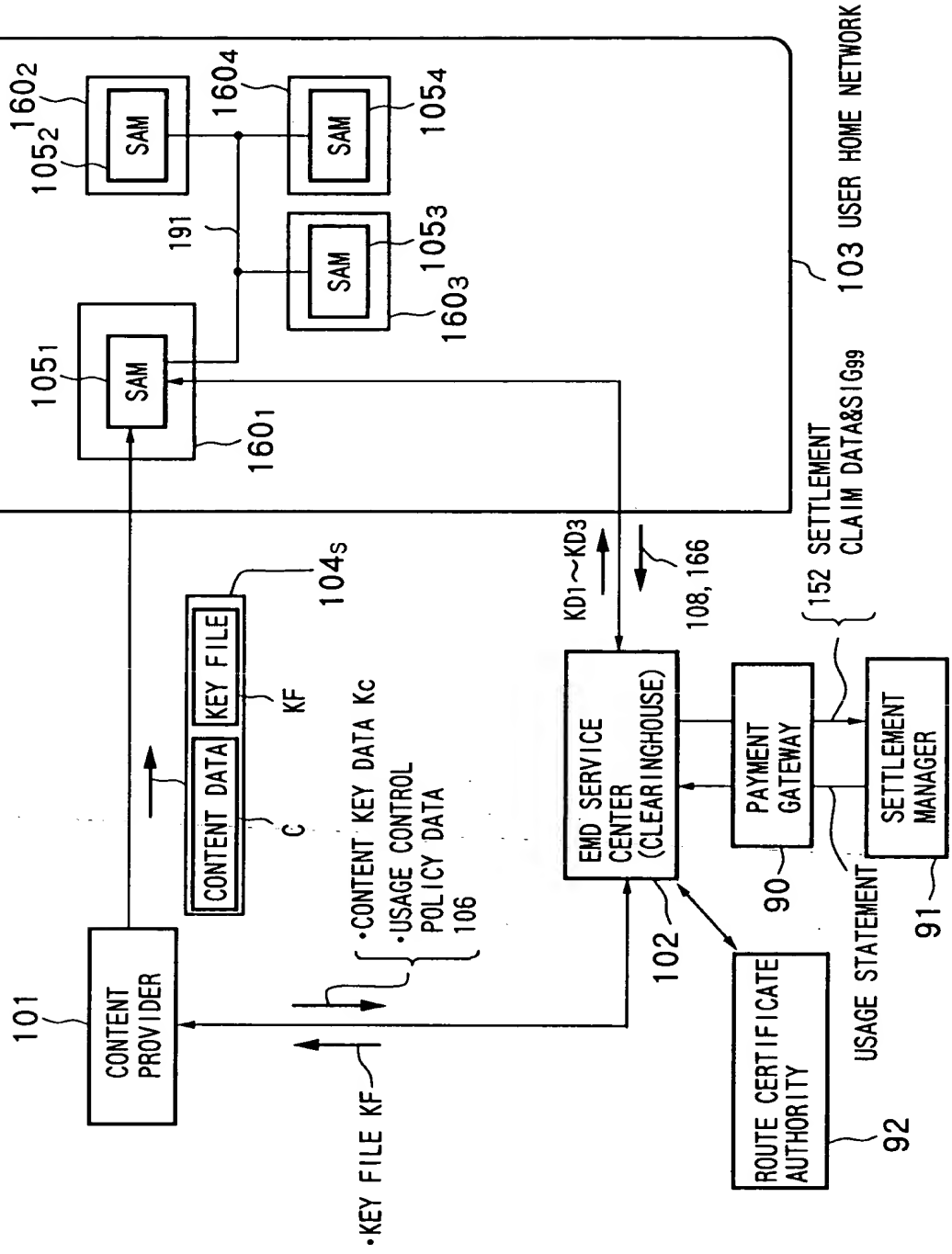

103 USER HOME NETWORK
SAM
1052
1602
1604
1054
1053
1603
191
1051
1601
152 SETTLEMENT CLAIM DATA&SIG99
KD1~KD3
108, 166
104S
KEY FILE
KF
CONTENT DATA
C
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
90
91
102
101
CONTENT PROVIDER
•KEY FILE KF
ROUTE CERTIFICATE AUTHORITY
92
USAGE STATEMENT

FIG.55

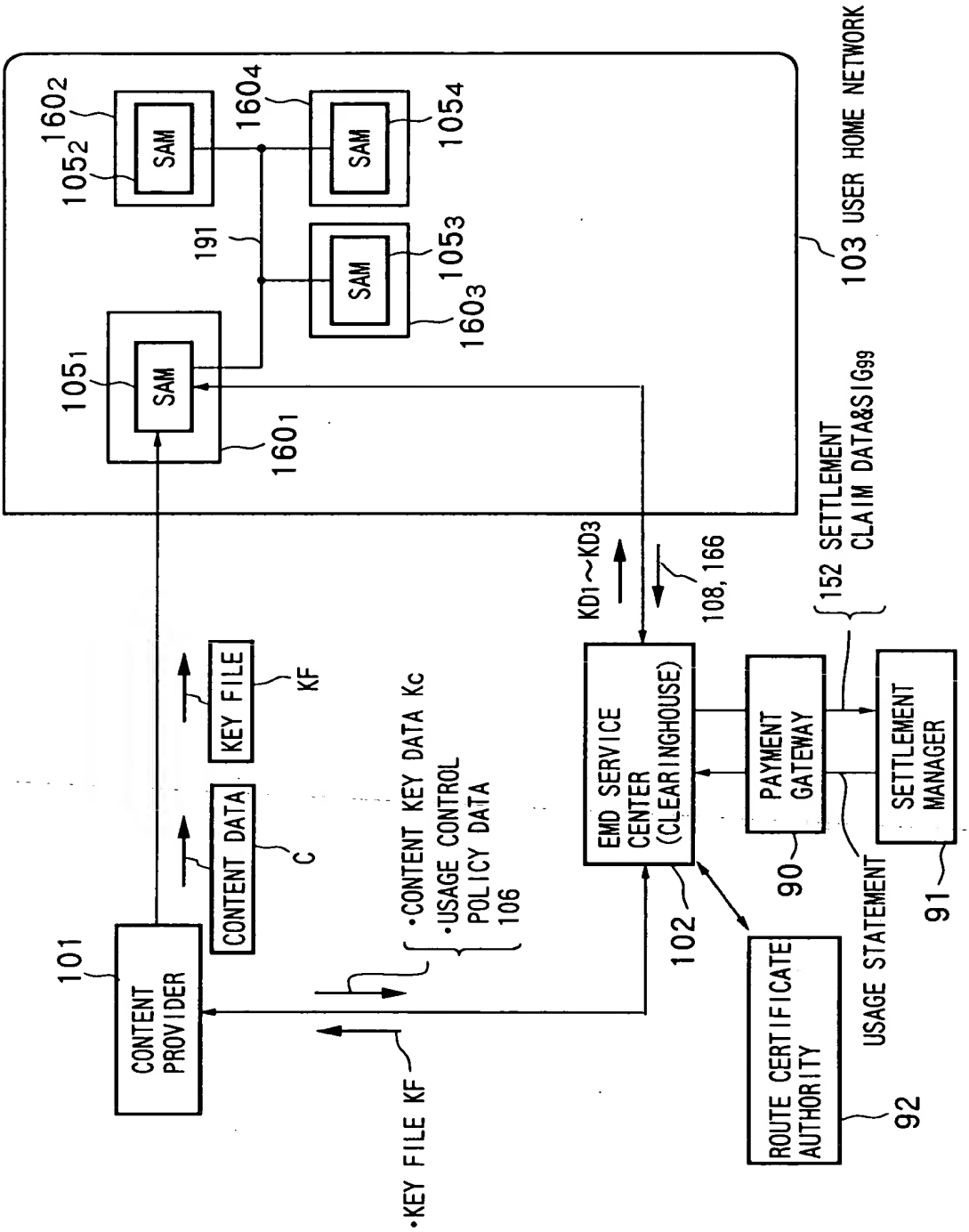

103 USER HOME NETWORK
SAM
1052
1602
1051
1601
1053
1603
1054
1604
191
101
CONTENT PROVIDER
CONTENT DATA
C
KEY FILE
KF
•KEY FILE KF
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
KD1~KD3
108, 166
EMD SERVICE CENTER (CLEARINGHOUSE)
102
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
152 SETTLEMENT CLAIM DATA&SIG99
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY
92

FIG.56

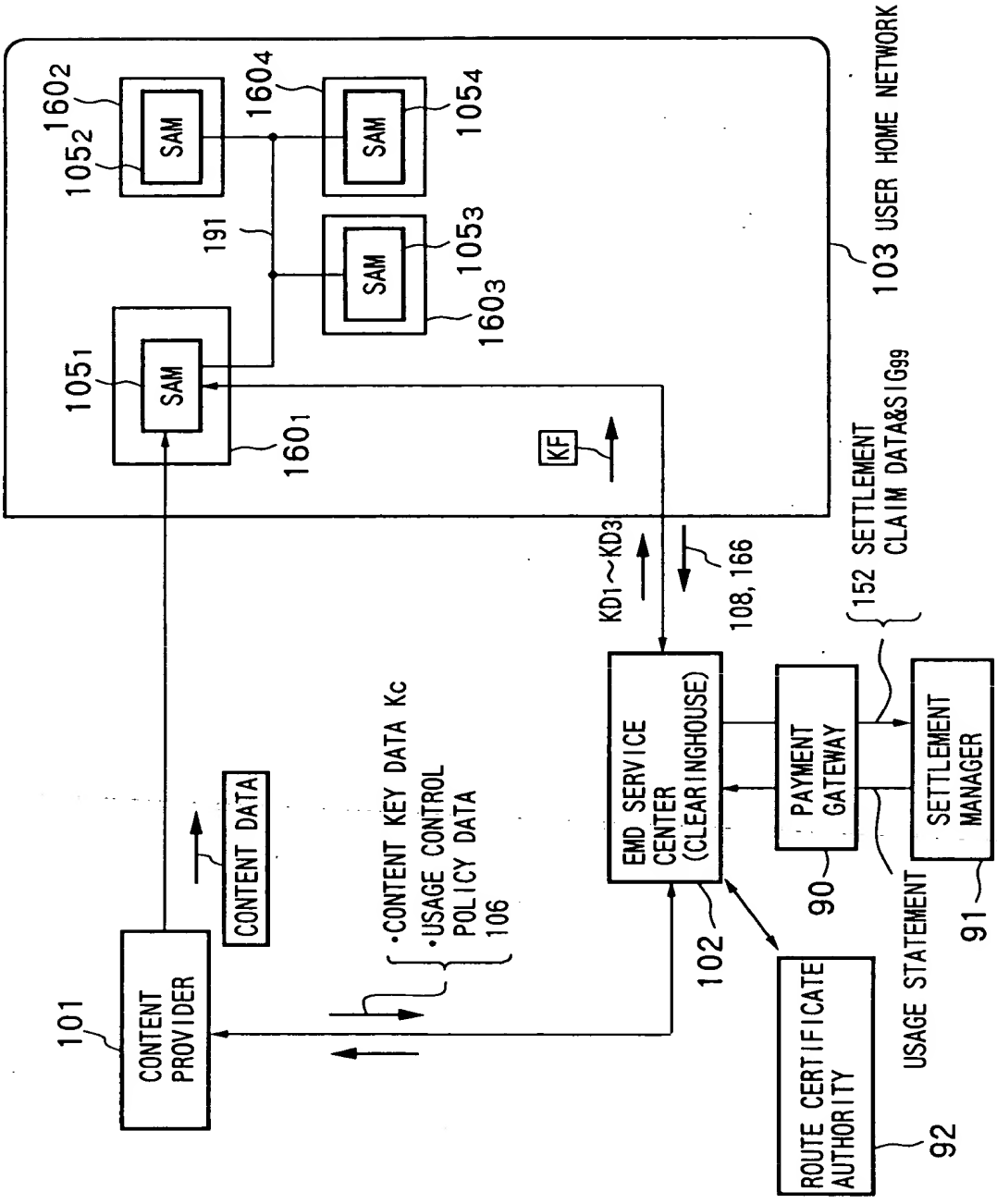

103 USER HOME NETWORK
SAM
SAM
SAM
SAM
1052
1602
1051
1601
1053
1603
1054
1604
191
KF
KD1~KD3
108, 166
152 SETTLEMENT CLAIM DATA&SIG99
CONTENT DATA
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
101
CONTENT PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
102
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY
92

FIG.57

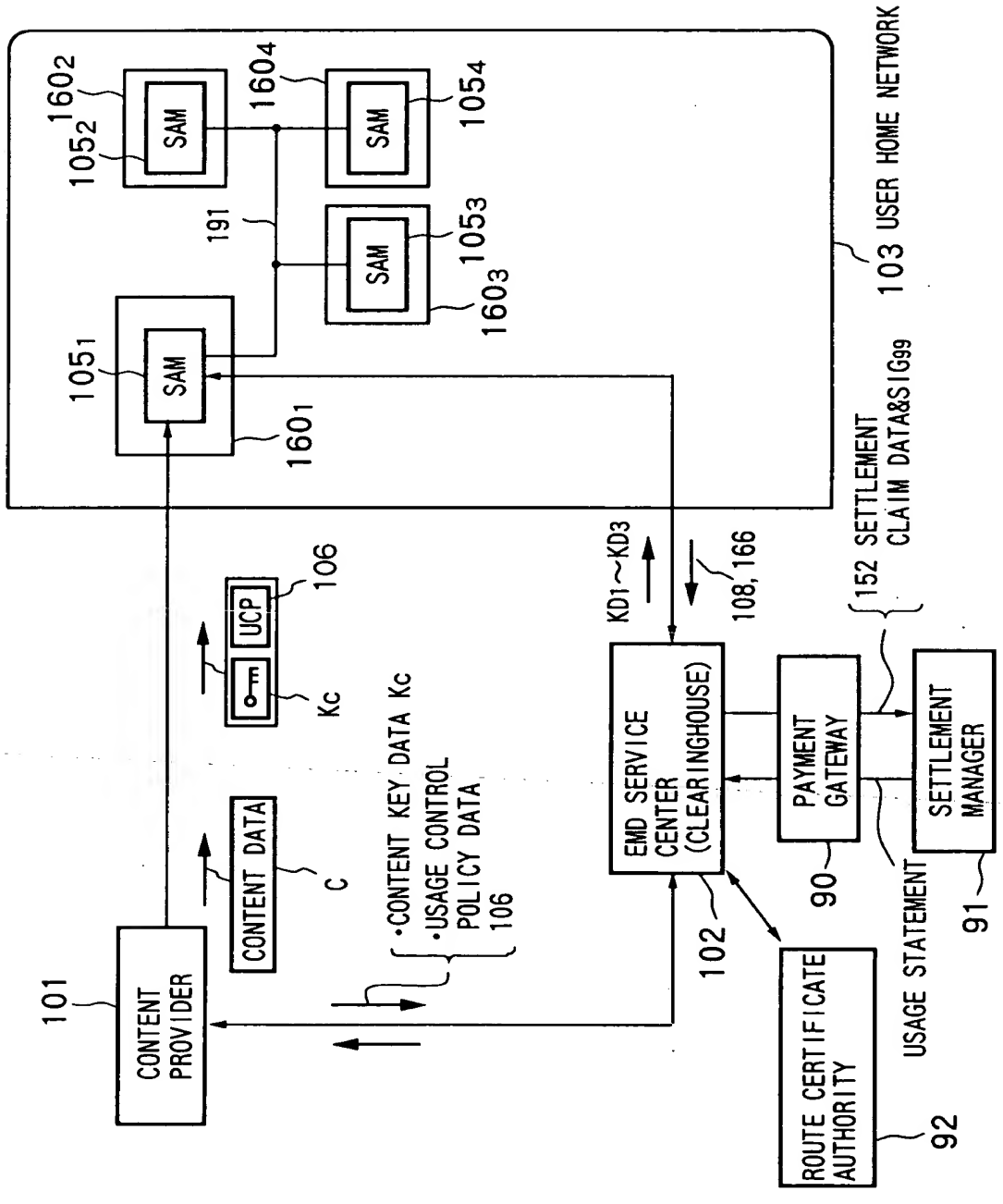

CONTENT PROVIDER
101
CONTENT DATA
C
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA
106
UCP
106
Kc
SAM
105_1
160_1
SAM
105_2
160_2
SAM
105_3
160_3
SAM
105_4
160_4
191
103 USER HOME NETWORK
KD1~KD3
108, 166
152 SETTLEMENT CLAIM DATA&SIG99
EMD SERVICE CENTER (CLEARINGHOUSE)
102
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
USAGE STATEMENT
ROUTE CERTIFICATE AUTHORITY
92

FIG.58

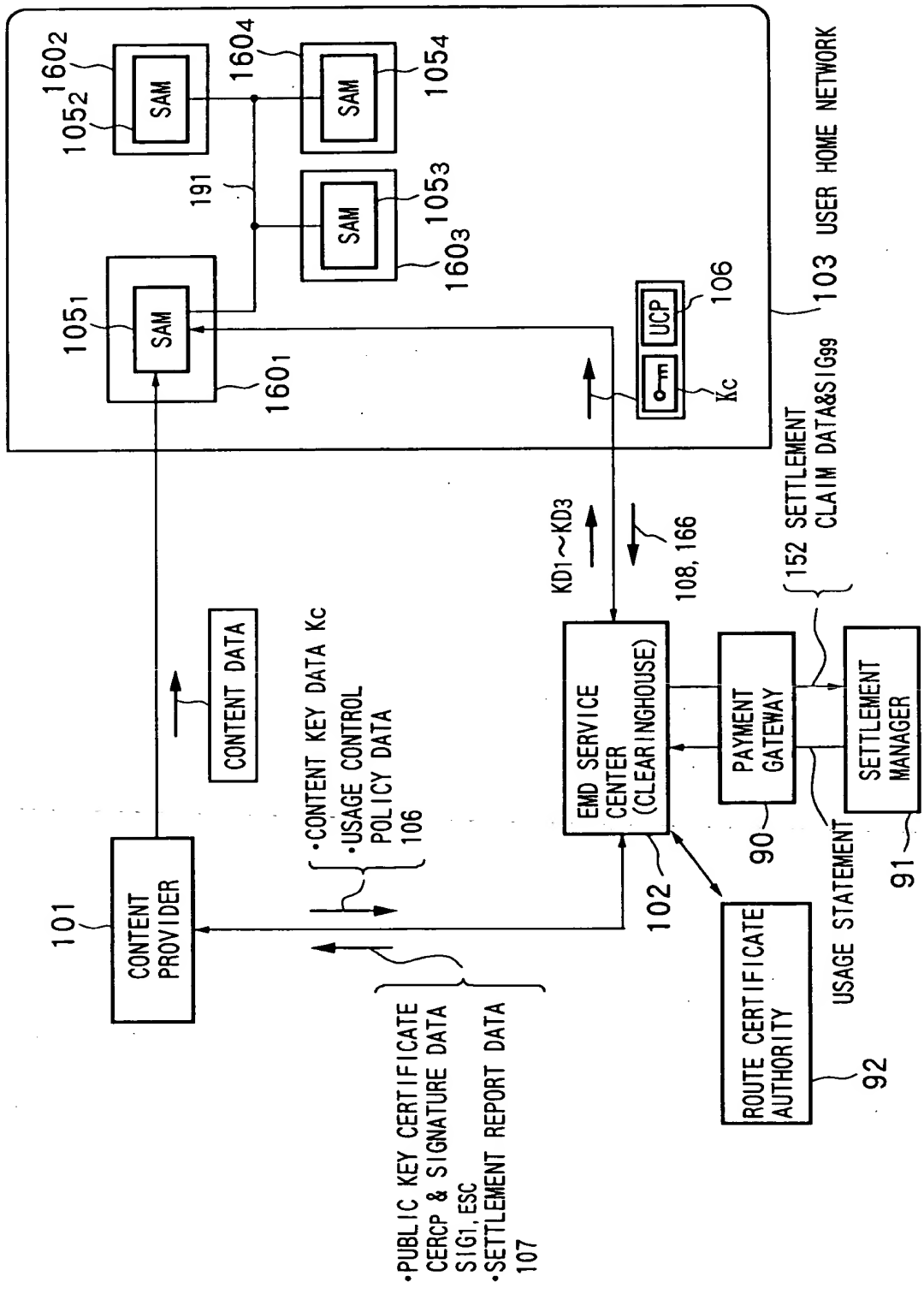

SAM
1052
1602
1604
1054
191
1053
1603
1051
1601
UCP
106
Kc
103 USER HOME NETWORK
152 SETTLEMENT CLAIM DATA&SIG99
KD1~KD3
108, 166
CONTENT DATA
•CONTENT KEY DATA Kc
•USAGE CONTROL POLICY DATA 106
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
101
CONTENT PROVIDER
102
90
91
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 107
ROUTE CERTIFICATE AUTHORITY
USAGE STATEMENT
92

FIG.59

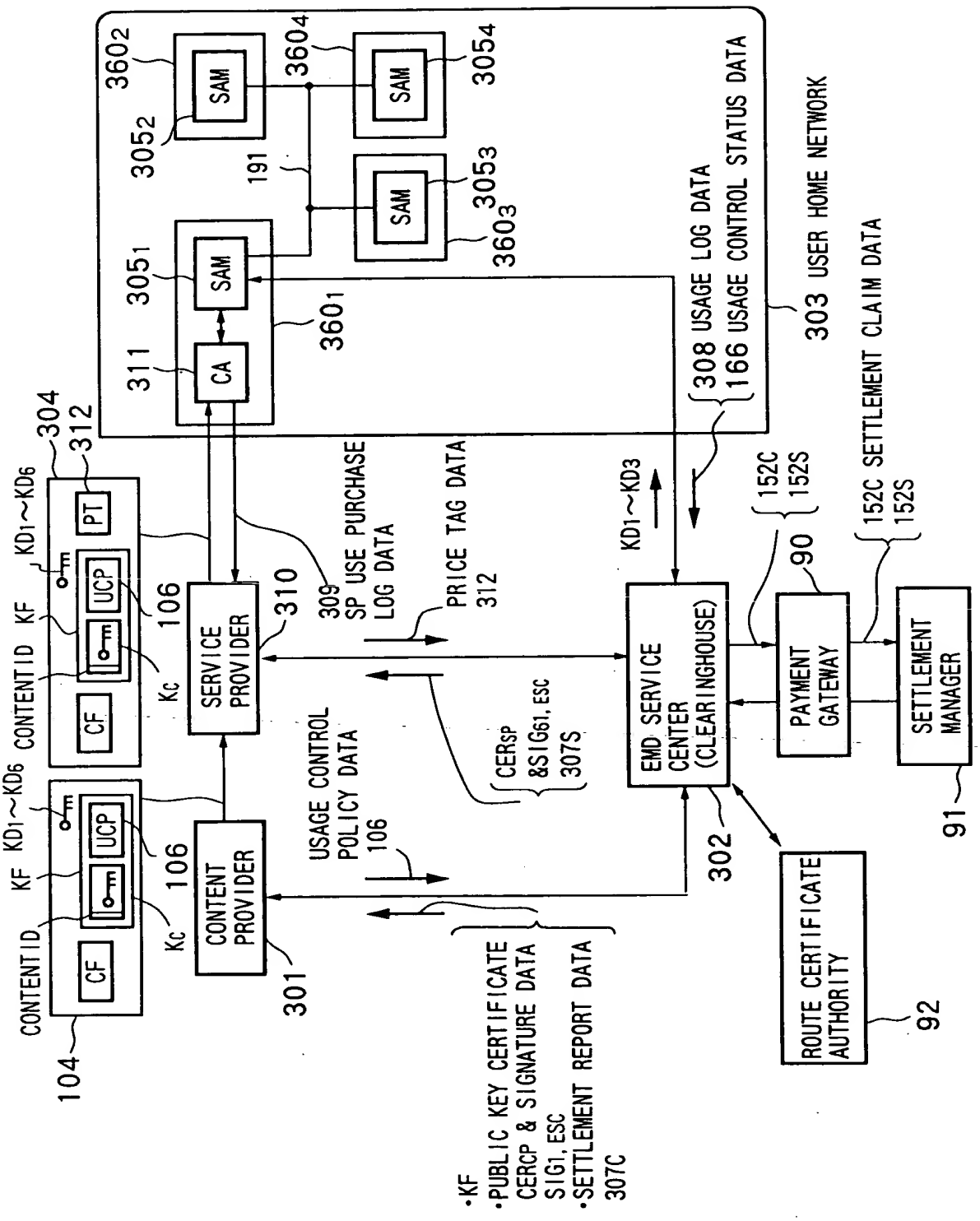

3602
3604
3054
3052
SAM
191
3053
3603
3051
3601
311
CA
304
312
PT
KD1~KD6
CONTENT ID
KF
UCP
CF
Kc
106
104
SERVICE PROVIDER
310
309 SP USE PURCHASE LOG DATA
PRICE TAG DATA 312
308 USAGE LOG DATA
166 USAGE CONTROL STATUS DATA
303 USER HOME NETWORK
KD1~KD3
152C
152S
152C SETTLEMENT CLAIM DATA
152S
90
PAYMENT GATEWAY
SETTLEMENT MANAGER
91
EMD SERVICE CENTER (CLEARINGHOUSE)
302
CONTENT PROVIDER
301
USAGE CONTROL POLICY DATA
106
CERSP &SIG61, ESC
307S
ROUTE CERTIFICATE AUTHORITY
92
•KF
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 307C

FIG.60

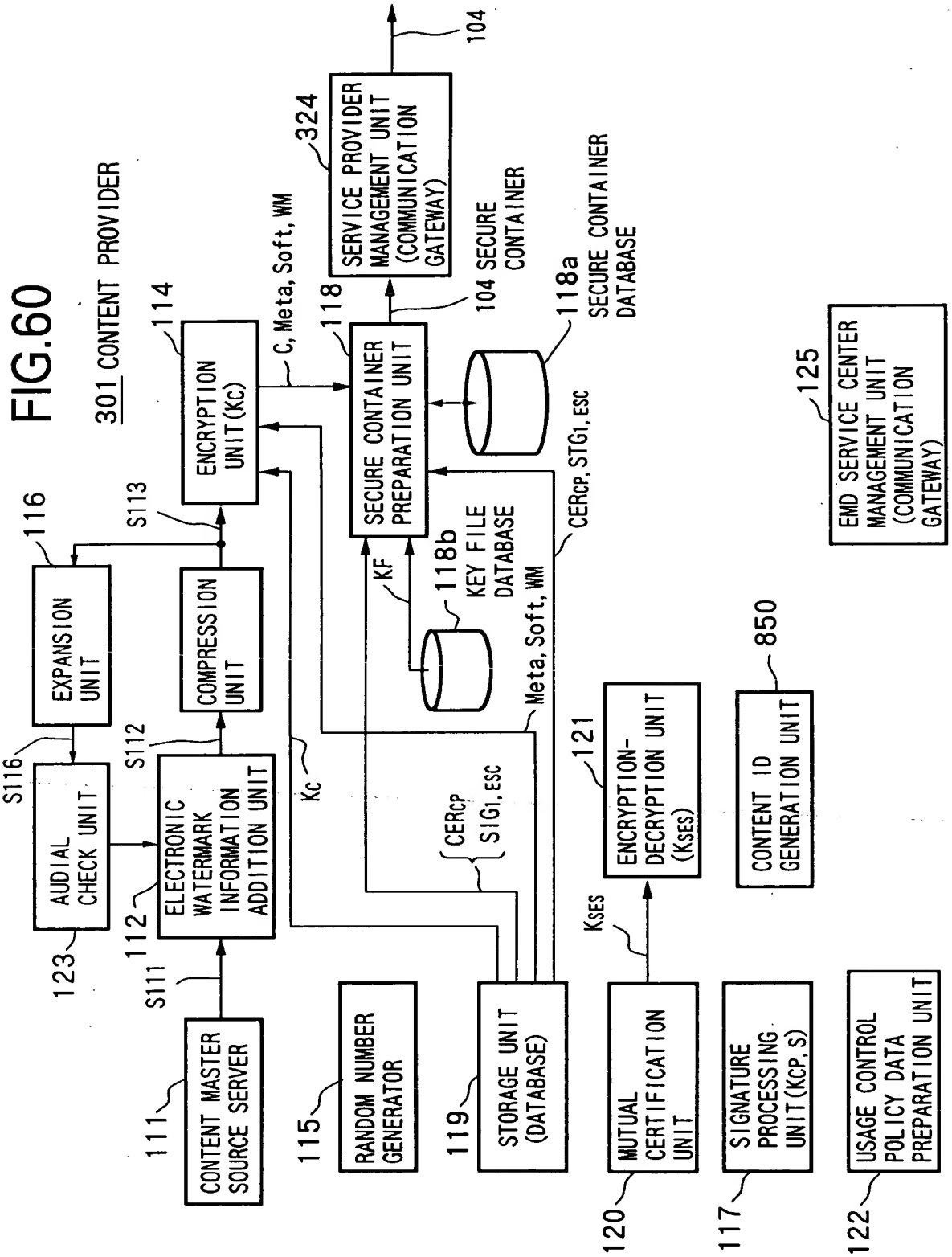

301 CONTENT PROVIDER
CONTENT MASTER SOURCE SERVER
111
AUDIAL CHECK UNIT
123
EXPANSION UNIT
116
ELECTRONIC WATERMARK INFORMATION ADDITION UNIT
112
COMPRESSION UNIT
ENCRYPTION UNIT(Kc)
114
RANDOM NUMBER GENERATOR
115
STORAGE UNIT (DATABASE)
119
MUTUAL CERTIFICATION UNIT
120
ENCRYPTION-DECRYPTION UNIT (KSES)
121
SIGNATURE PROCESSING UNIT(KCP, S)
117
CONTENT ID GENERATION UNIT
850
USAGE CONTROL POLICY DATA PREPARATION UNIT
122
SECURE CONTAINER PREPARATION UNIT
118
KEY FILE DATABASE
118b
SECURE CONTAINER DATABASE
118a
SERVICE PROVIDER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
324
EMD SERVICE CENTER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
125
104
104 SECURE CONTAINER
S111
S112
S113
S116
KC
KF
KSES
C, Meta, Soft, WM
Meta, Soft, WM
CERCP, SIG1, ESC
CERCP
SIG1, ESC

FIG.61

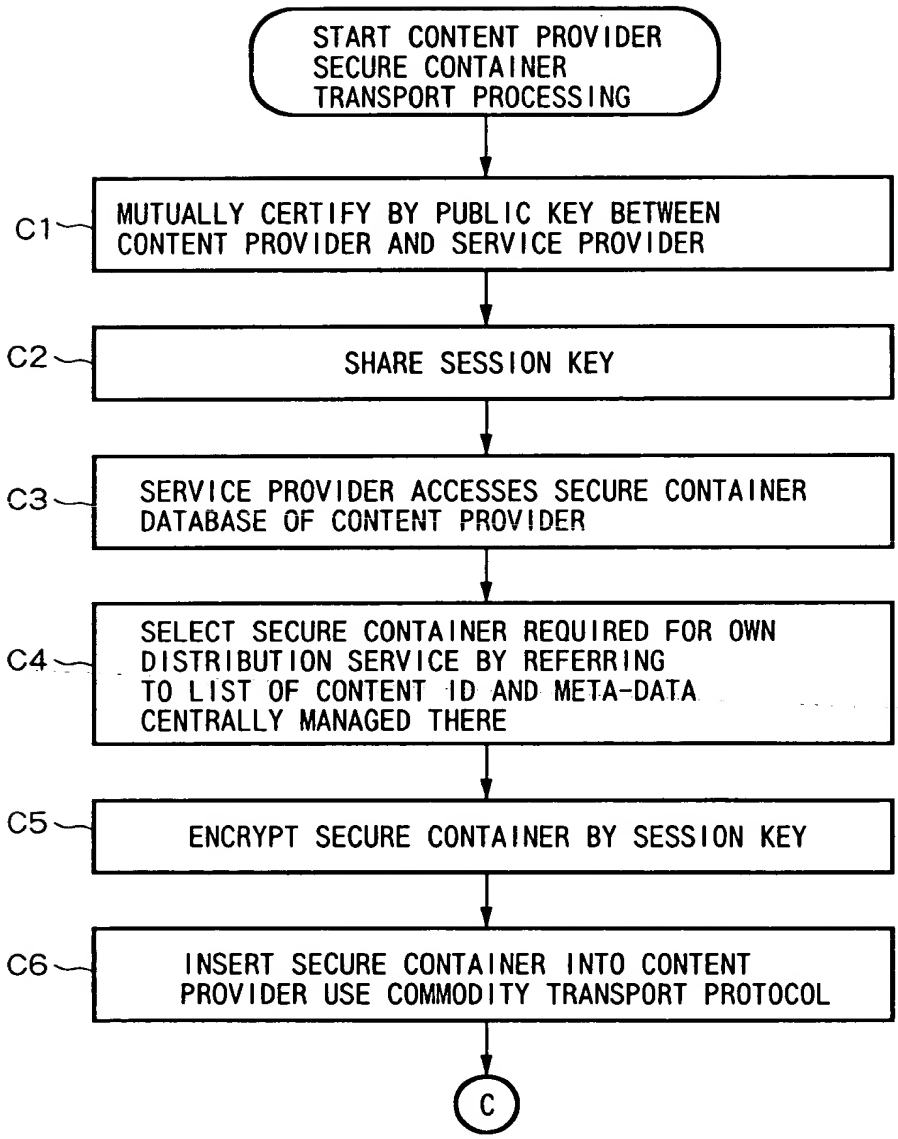


FIG.62

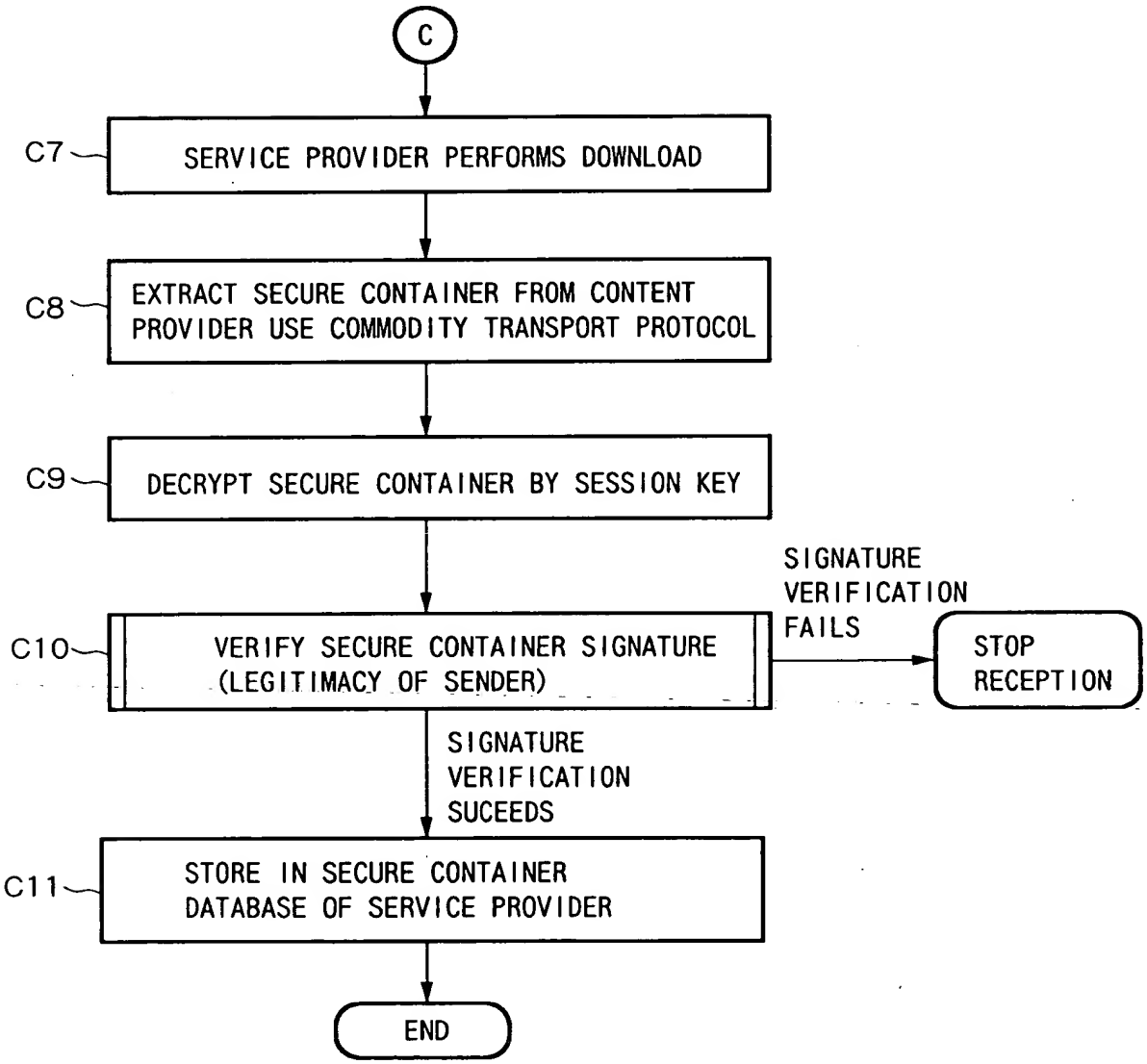

C
C7
SERVICE PROVIDER PERFORMS DOWNLOAD
C8
EXTRACT SECURE CONTAINER FROM CONTENT PROVIDER USE COMMODITY TRANSPORT PROTOCOL
C9
DECRYPT SECURE CONTAINER BY SESSION KEY
C10
VERIFY SECURE CONTAINER SIGNATURE (LEGITIMACY OF SENDER)
SIGNATURE VERIFICATION FAILS
STOP RECEPTION
SIGNATURE VERIFICATION SUCEEDS
C11
STORE IN SECURE CONTAINER DATABASE OF SERVICE PROVIDER
END

FIG.63

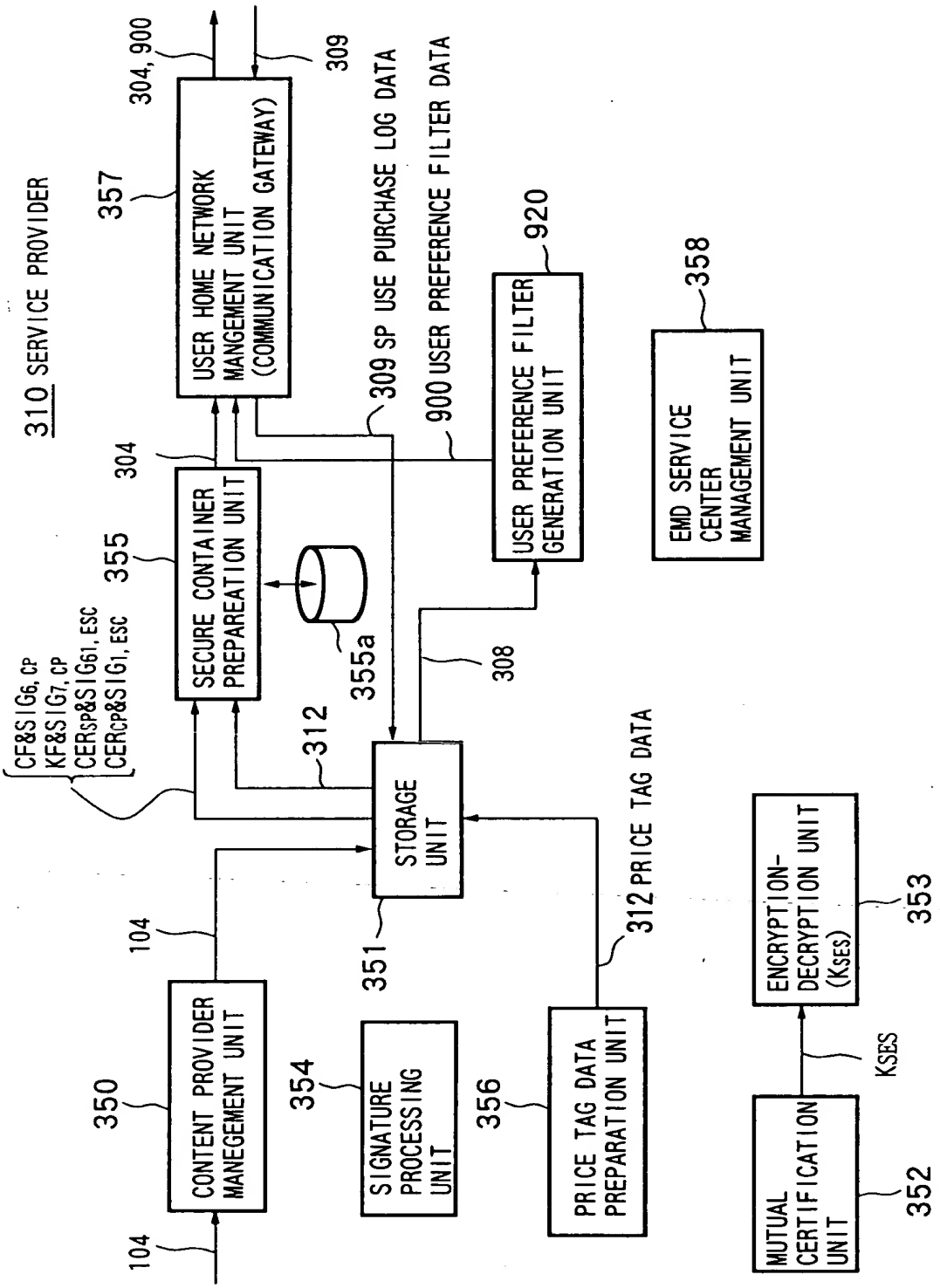

310 SERVICE PROVIDER
CF&SIG6, CP
KF&SIG7, CP
CERSP&SIG61, ESC
CERCP&SIG1, ESC
CONTENT PROVIDER MANEGEMENT UNIT
350
104
104
SIGNATURE PROCESSING UNIT
354
SECURE CONTAINER PREPAREATION UNIT
355
304
355a
312
STORAGE UNIT
351
USER HOME NETWORK MANGEMENT UNIT (COMMUNICATION GATEWAY)
357
304, 900
309
309 SP USE PURCHASE LOG DATA
900 USER PREFERENCE FILTER DATA
USER PREFERENCE FILTER GENERATION UNIT
920
308
EMD SERVICE CENTER MANAGEMENT UNIT
358
312 PRICE TAG DATA
PRICE TAG DATA PREPARATION UNIT
356
ENCRYPTION-DECRYPTION UNIT (KSES)
353
KSES
MUTUAL CERTIFICATION UNIT
352

FIG.64

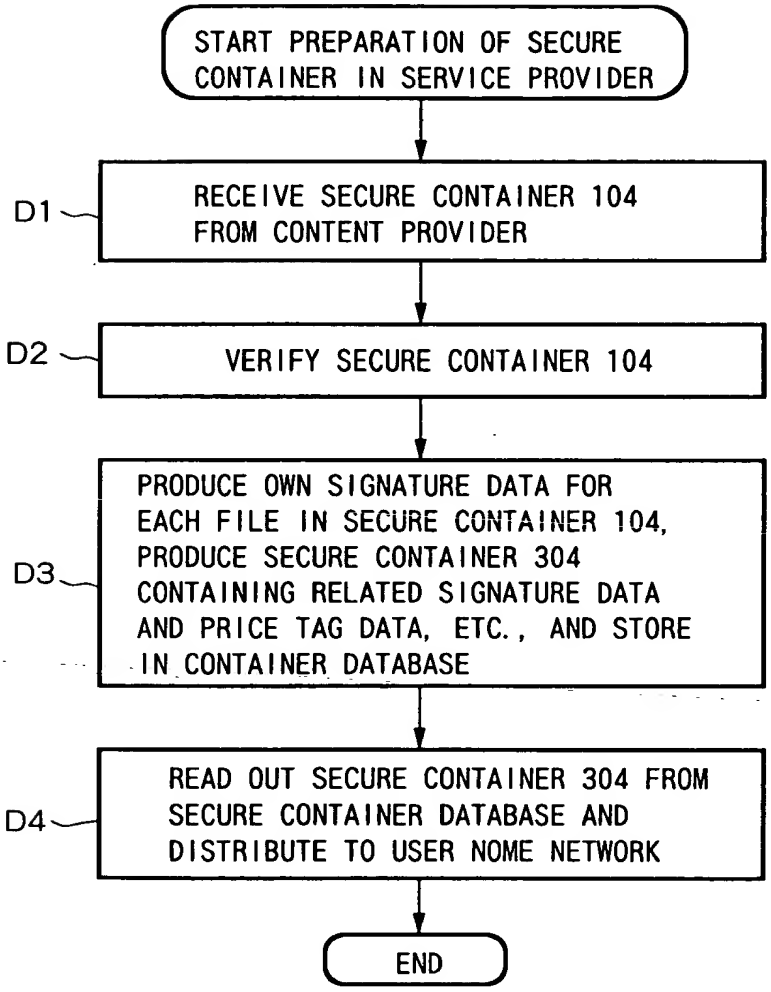


FIG.65A

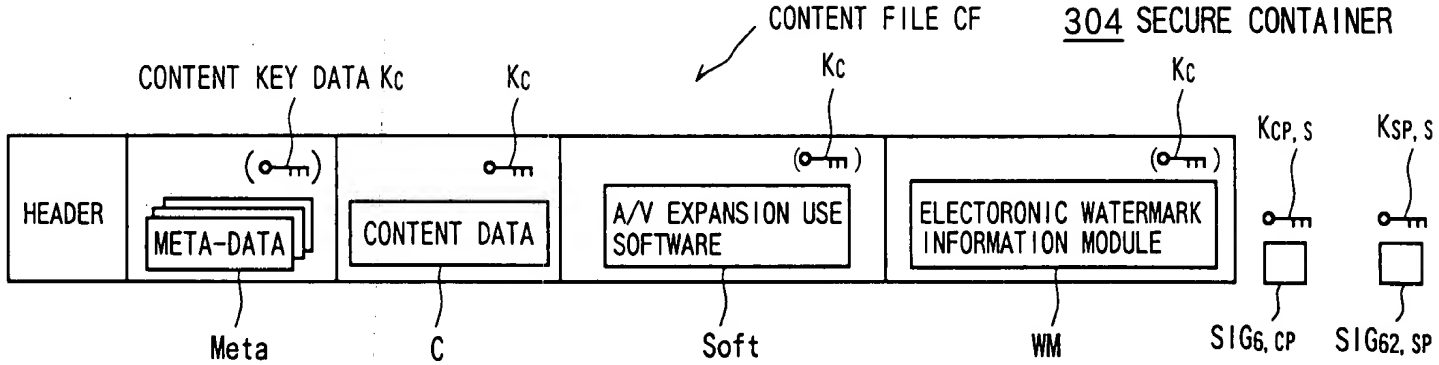


FIG.65B

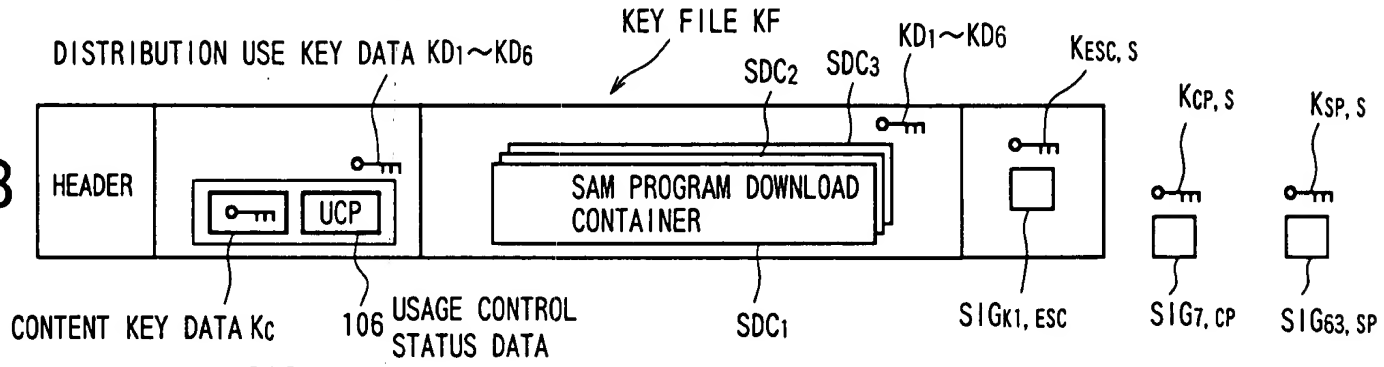


FIG.65C

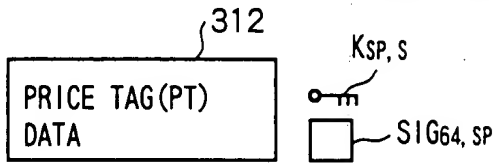
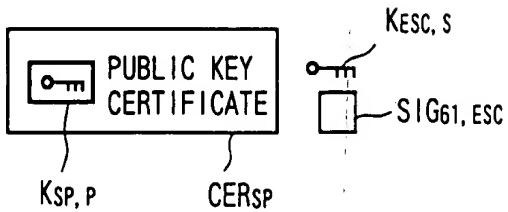


FIG.65D



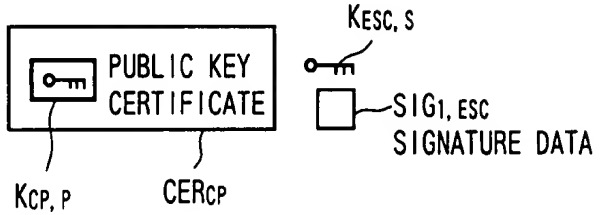


FIG.66

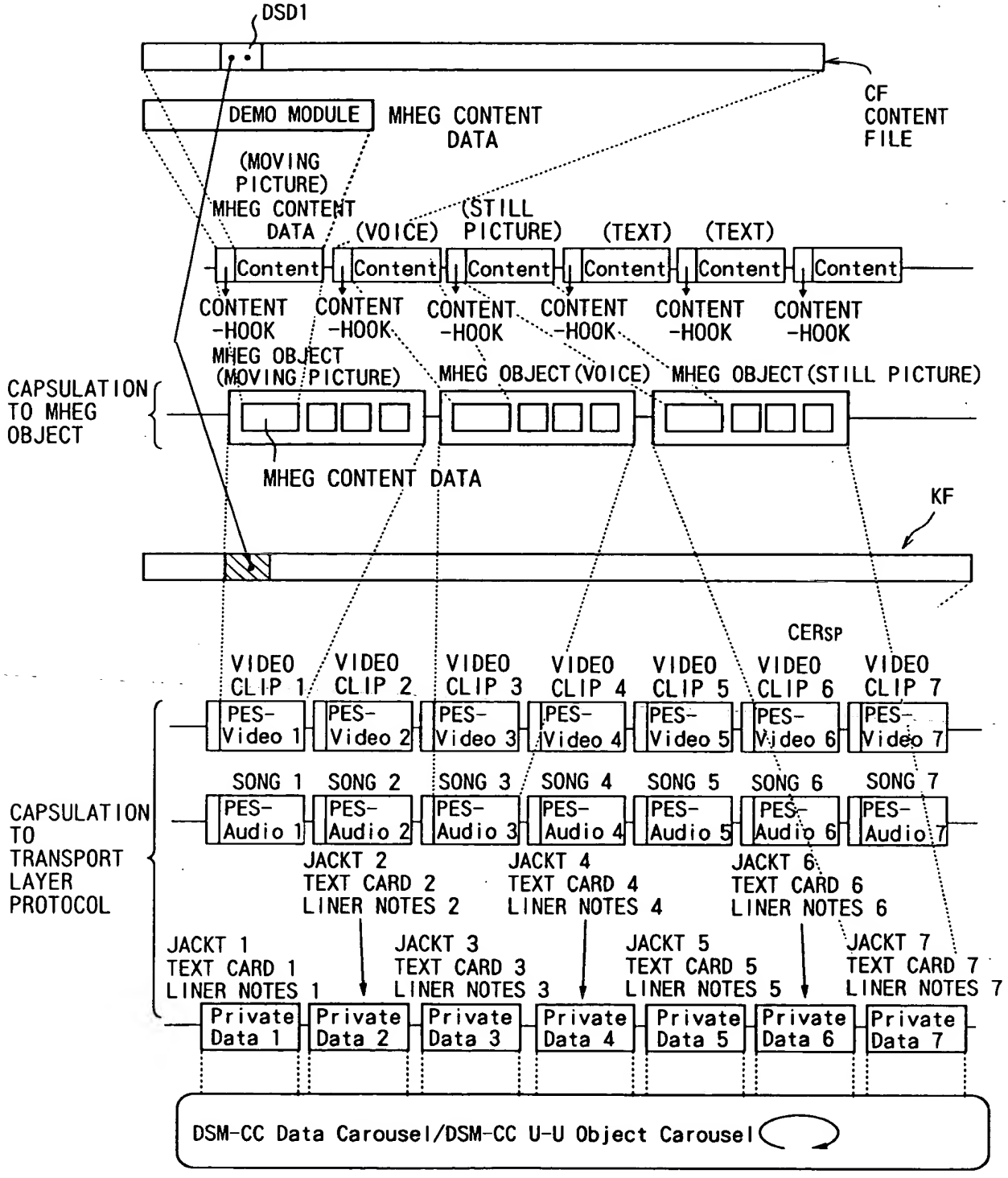

DSD1
CF CONTENT FILE
DEMO MODULE
MHEG CONTENT DATA
(MOVING PICTURE) MHEG CONTENT DATA
(VOICE)
(STILL PICTURE)
(TEXT)
(TEXT)
Content
CONTENT -HOOK
MHEG OBJECT (MOVING PICTURE)
MHEG OBJECT (VOICE)
MHEG OBJECT (STILL PICTURE)
CAPSULATION TO MHEG OBJECT
MHEG CONTENT DATA
KF
CERSP
VIDEO CLIP 1
VIDEO CLIP 2
VIDEO CLIP 3
VIDEO CLIP 4
VIDEO CLIP 5
VIDEO CLIP 6
VIDEO CLIP 7
PES-Video 1
PES-Video 2
PES-Video 3
PES-Video 4
PES-Video 5
PES-Video 6
PES-Video 7
SONG 1
SONG 2
SONG 3
SONG 4
SONG 5
SONG 6
SONG 7
PES-Audio 1
PES-Audio 2
PES-Audio 3
PES-Audio 4
PES-Audio 5
PES-Audio 6
PES-Audio 7
CAPSULATION TO TRANSPORT LAYER PROTOCOL
JACKT 1 TEXT CARD 1 LINER NOTES 1
JACKT 2 TEXT CARD 2 LINER NOTES 2
JACKT 3 TEXT CARD 3 LINER NOTES 3
JACKT 4 TEXT CARD 4 LINER NOTES 4
JACKT 5 TEXT CARD 5 LINER NOTES 5
JACKT 6 TEXT CARD 6 LINER NOTES 6
JACKT 7 TEXT CARD 7 LINER NOTES 7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

FIG.67

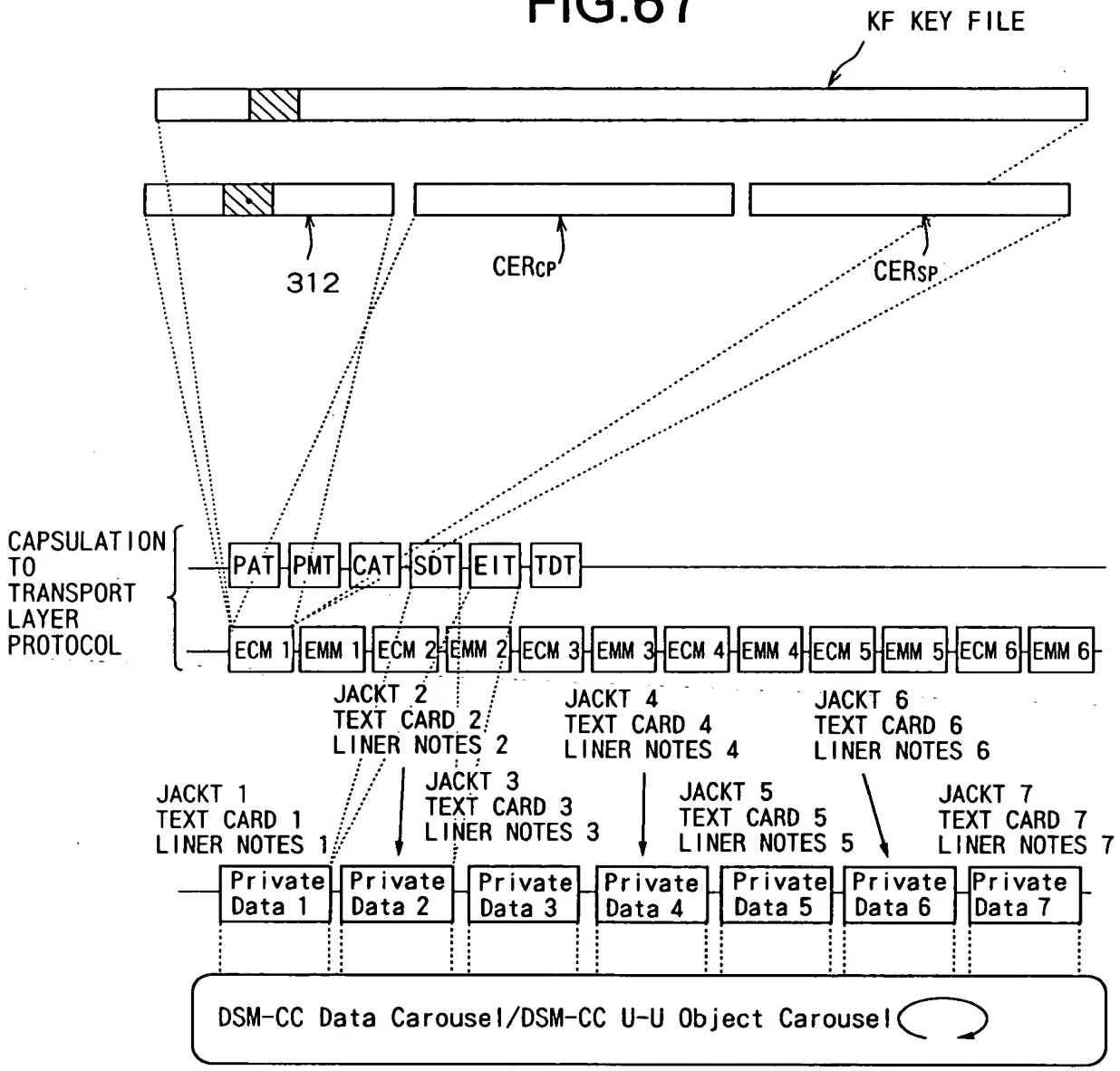

KF KEY FILE
312
CERCP
CERSP
CAPSULATION TO TRANSPORT LAYER PROTOCOL
PAT
PMT
CAT
SDT
EIT
TDT
ECM 1
EMM 1
ECM 2
EMM 2
ECM 3
EMM 3
ECM 4
EMM 4
ECM 5
EMM 5
ECM 6
EMM 6
JACKT 1
TEXT CARD 1
LINER NOTES 1
JACKT 2
TEXT CARD 2
LINER NOTES 2
JACKT 3
TEXT CARD 3
LINER NOTES 3
JACKT 4
TEXT CARD 4
LINER NOTES 4
JACKT 5
TEXT CARD 5
LINER NOTES 5
JACKT 6
TEXT CARD 6
LINER NOTES 6
JACKT 7
TEXT CARD 7
LINER NOTES 7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

FIG.68

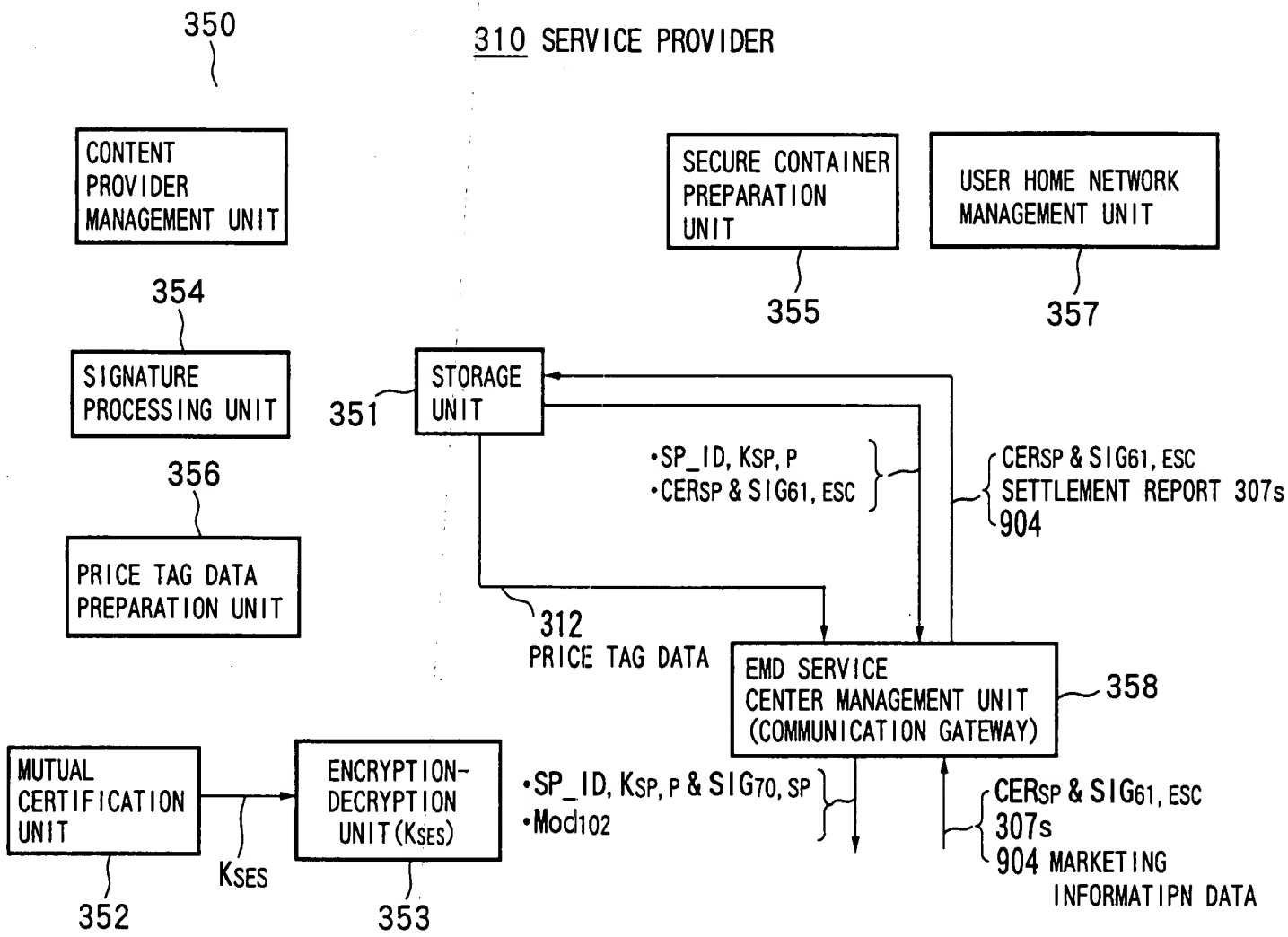


FIG.69

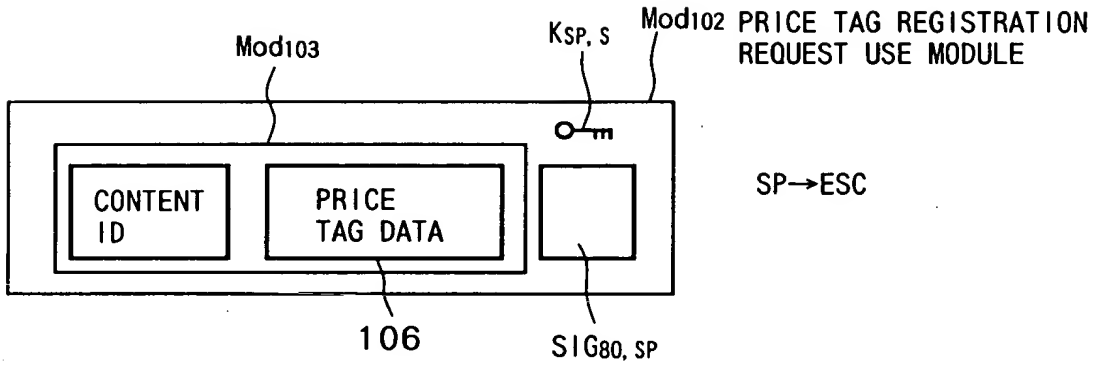

Mod103
KSP, S
Mod102 PRICE TAG REGISTRATION REQUEST USE MODULE
CONTENT ID
PRICE TAG DATA
SP→ESC
106
SIG80, SP

FIG.70

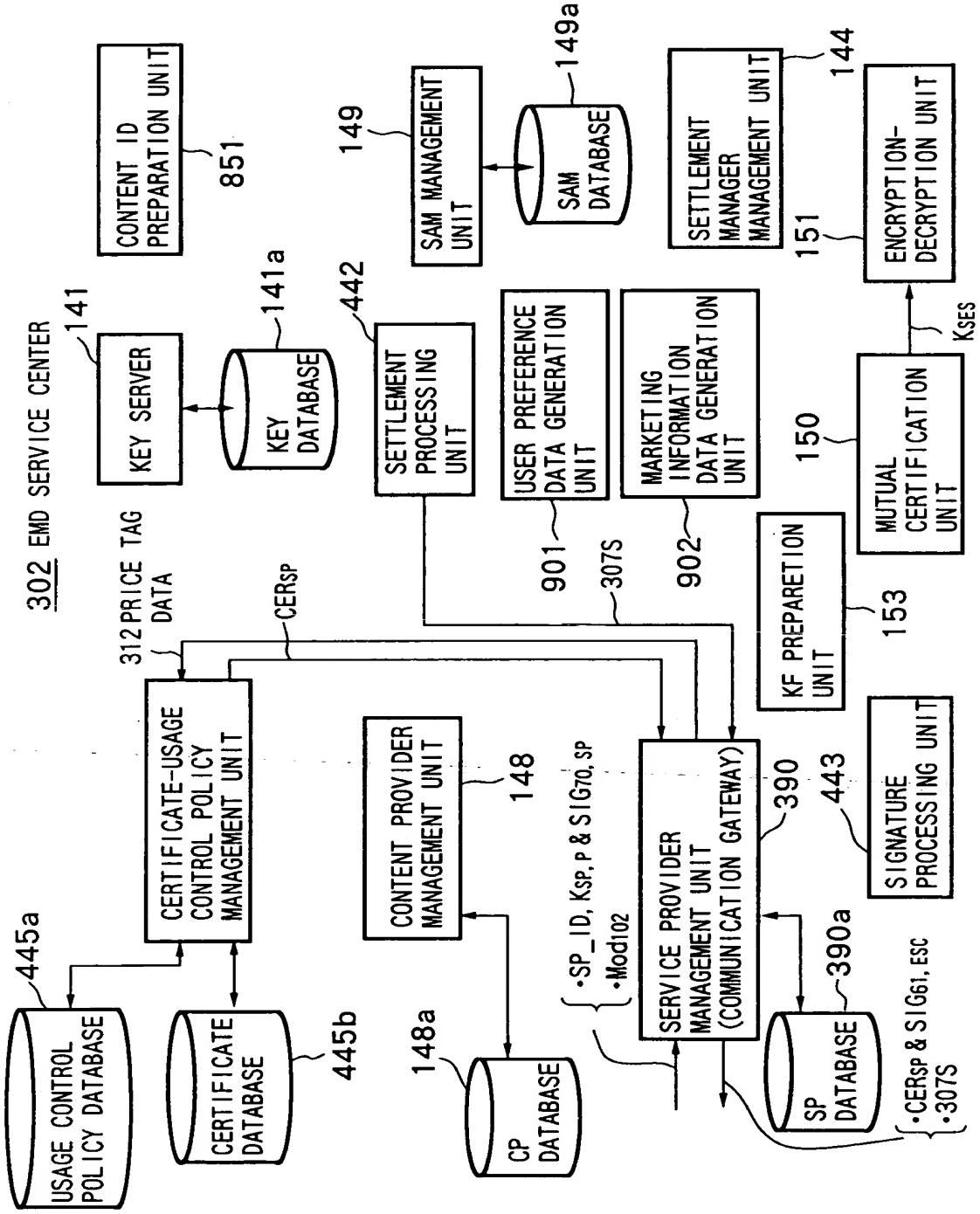


FIG.71

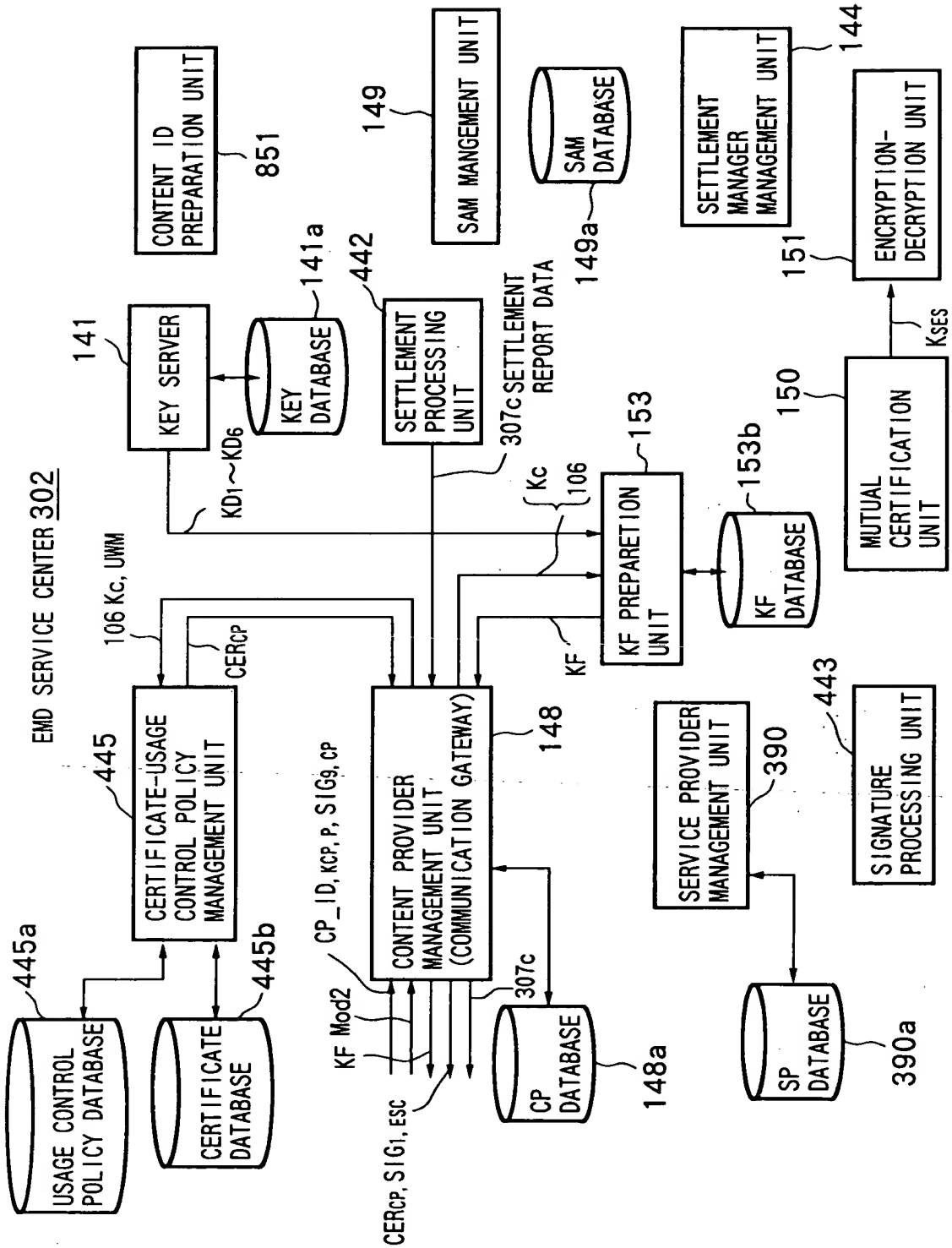

EMD SERVICE CENTER 302
CONTENT ID PREPARATION UNIT
851
SAM MANGEMENT UNIT
149
SAM DATABASE
149a
SETTLEMENT MANAGER MANAGEMENT UNIT
144
ENCRYPTION-DECRYPTION UNIT
151
KEY SERVER
141
KEY DATABASE
141a
SETTLEMENT PROCESSING UNIT
442
307c SETTLEMENT REPORT DATA
KD1~KD6
Kc
106
KF PREPARETION UNIT
153
153b
KF DATABASE
MUTUAL CERTIFICATION UNIT
150
KSES
106 Kc, UWM
CERCP
CERTIFICATE-USAGE CONTROL POLICY MANAGEMENT UNIT
445
CONTENT PROVIDER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
148
CP_ID, KCP, P, SIG9, CP
KF
KF Mod2
CERCP, SIG1, ESC
307c
SERVICE PROVIDER MANAGEMENT UNIT
390
443
SIGNATURE PROCESSING UNIT
445a
USAGE CONTROL POLICY DATABASE
445b
CERTIFICATE DATABASE
CP DATABASE
148a
SP DATABASE
390a

FIG.72

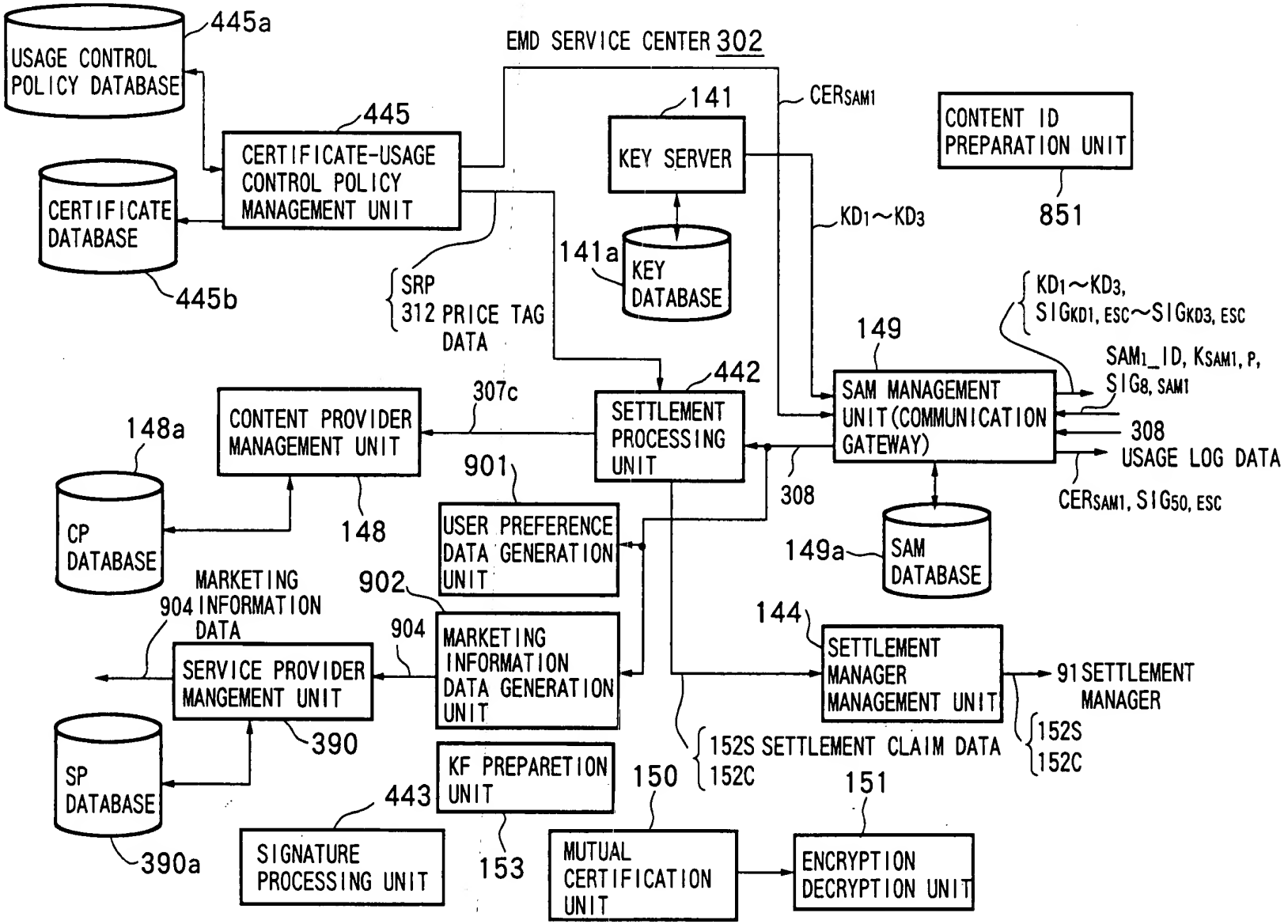

445a
USAGE CONTROL POLICY DATABASE
EMD SERVICE CENTER 302
141
CERSAM1
CONTENT ID PREPARATION UNIT
445
CERTIFICATE-USAGE CONTROL POLICY MANAGEMENT UNIT
KEY SERVER
CERTIFICATE DATABASE
KD1~KD3
851
141a
KEY DATABASE
445b
SRP
312 PRICE TAG DATA
KD1~KD3,
SIGKD1, ESC~SIGKD3, ESC
149
SAM1_ID, KSAM1, P,
SIG8, SAM1
442
307c
SAM MANAGEMENT UNIT(COMMUNICATION GATEWAY)
148a
CONTENT PROVIDER MANAGEMENT UNIT
SETTLEMENT PROCESSING UNIT
308
USAGE LOG DATA
901
CERSAM1, SIG50, ESC
CP DATABASE
148
USER PREFERENCE DATA GENERATION UNIT
308
149a
SAM DATABASE
MARKETING
904 INFORMATION DATA
902
144
904
MARKETING INFORMATION DATA GENERATION UNIT
SETTLEMENT MANAGER MANAGEMENT UNIT
91 SETTLEMENT MANAGER
SERVICE PROVIDER MANGEMENT UNIT
390
152S SETTLEMENT CLAIM DATA
152C
152S
152C
SP DATABASE
KF PREPARETION UNIT
150
151
443
SIGNATURE PROCESSING UNIT
153
MUTUAL CERTIFICATION UNIT
ENCRYPTION DECRYPTION UNIT
390a

FIG.73

CONTENT OF USAGE LOG DATA 308

IDENTIFIER Content_ID
IDENTIFIER CP_ID
IDENTIFIER SP_ID
SIGNAL PARAMETER DATA OF CONTENT DATA C
COMPRESSION METHOD OF CONTENT DATA C
IDENTIFIER MEDIA_ID OF STORAGE MEDIA
IDENTIFIER SAM_ID
USER_ID OF USER

FIG.74

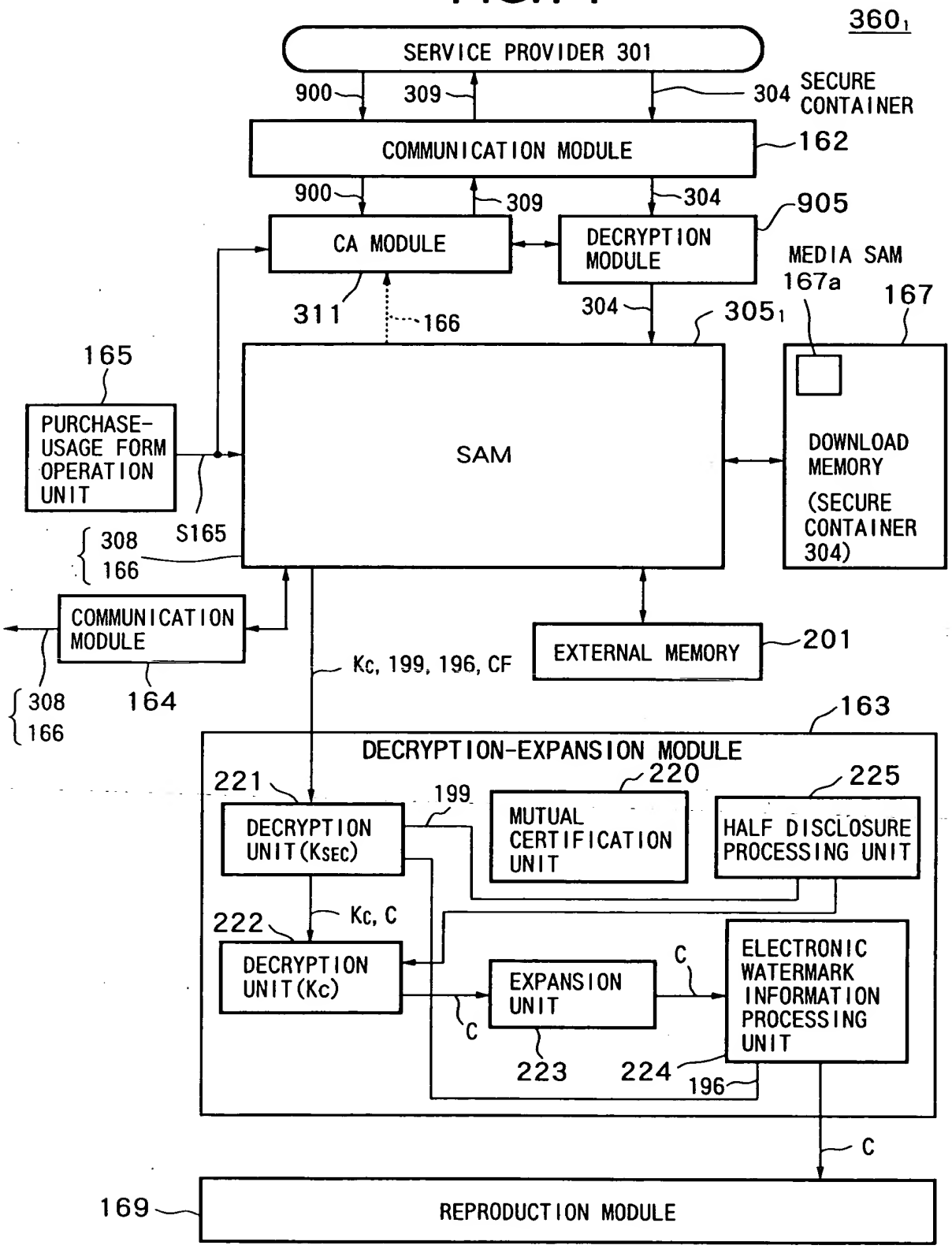

360₁
SERVICE PROVIDER 301
900
309
304 SECURE CONTAINER
COMMUNICATION MODULE
162
900
309
304
905
CA MODULE
DECRYPTION MODULE
MEDIA SAM
167a
167
311
166
304
305₁
165
PURCHASE-USAGE FORM OPERATION UNIT
SAM
DOWNLOAD MEMORY (SECURE CONTAINER 304)
S165
308
166
COMMUNICATION MODULE
EXTERNAL MEMORY
201
Kc, 199, 196, CF
308
166
164
163
DECRYPTION-EXPANSION MODULE
221
199
220
225
DECRYPTION UNIT(KSEC)
MUTUAL CERTIFICATION UNIT
HALF DISCLOSURE PROCESSING UNIT
Kc, C
222
DECRYPTION UNIT(Kc)
EXPANSION UNIT
C
ELECTRONIC WATERMARK INFORMATION PROCESSING UNIT
C
223
224
196
C
169
REPRODUCTION MODULE

FIG.75

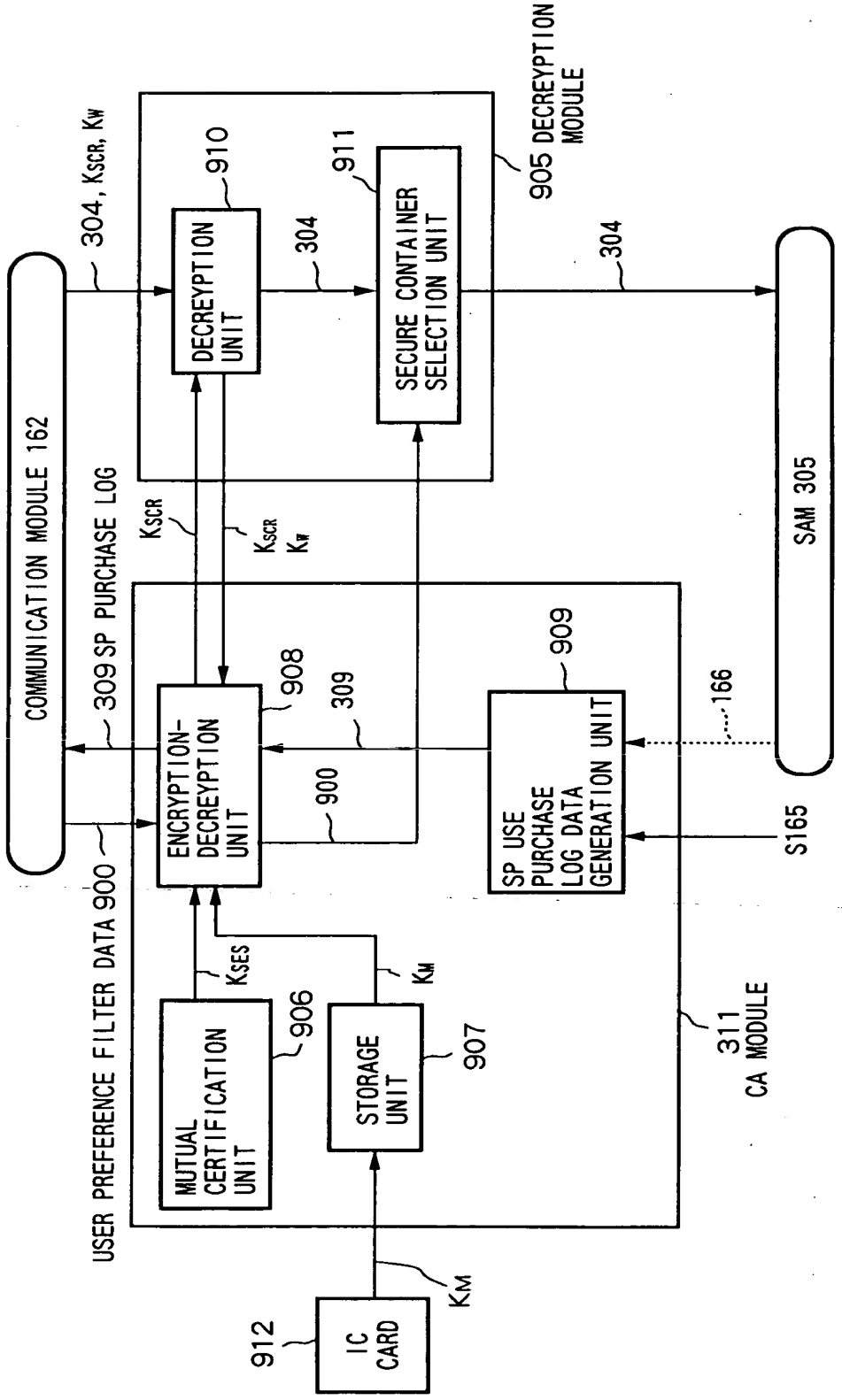

COMMUNICATION MODULE 162
304, KSCR, KW
DECREYPTION UNIT
910
304
SECURE CONTAINER SELECTION UNIT
911
905 DECREYPTION MODULE
304
SAM 305
KSCR
KSCR
KW
309 SP PURCHASE LOG
908
309
900
ENCRYPTION-DECREYPTION UNIT
909
166
SP USE PURCHASE LOG DATA GENERATION UNIT
S165
USER PREFERENCE FILTER DATA 900
KSES
KM
906
MUTUAL CERTIFICATION UNIT
907
STORAGE UNIT
311
CA MODULE
912
IC CARD
KM

FIG.76

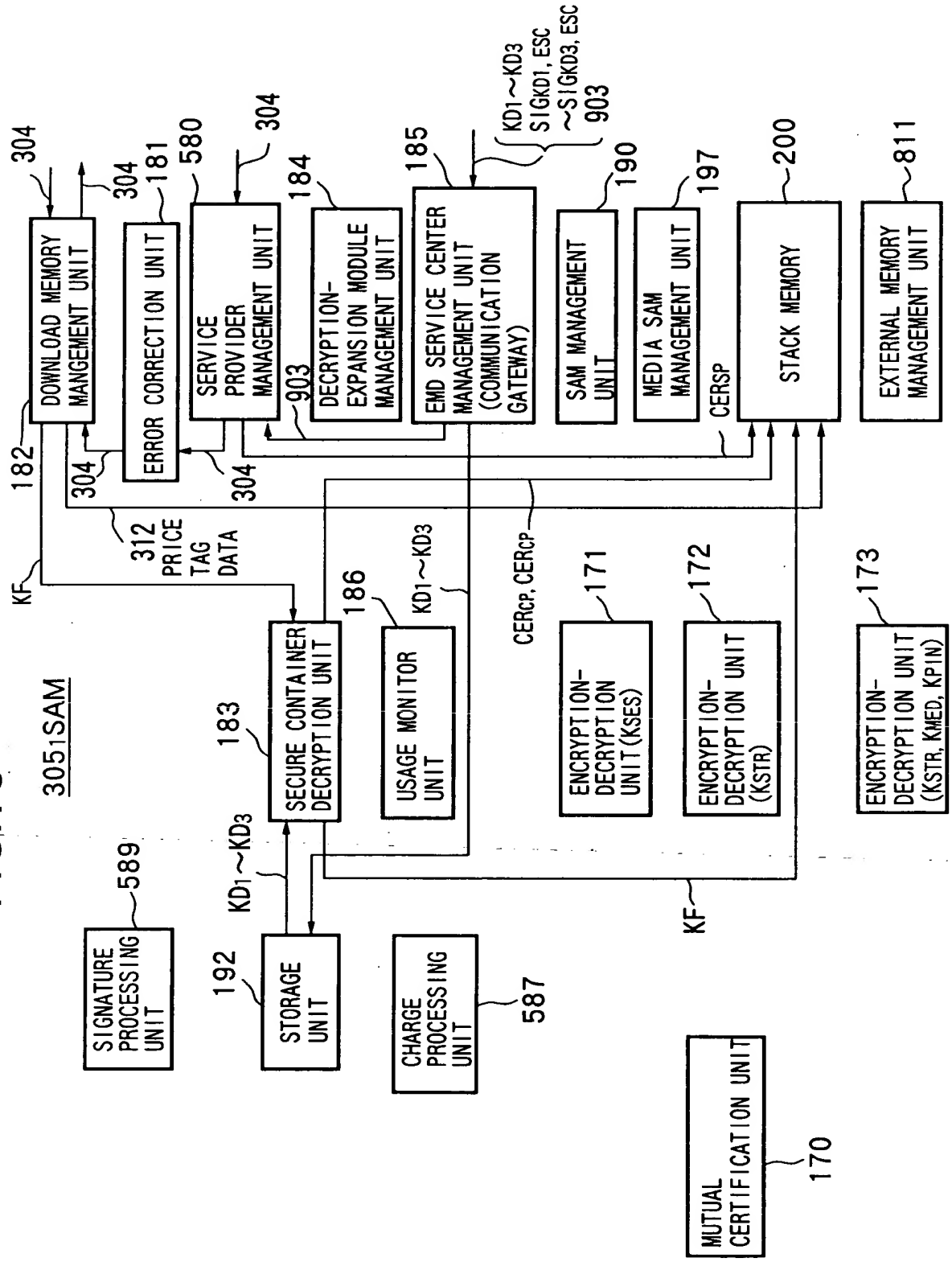

3051SAM
DOWNLOAD MEMORY MANGEMENT UNIT
ERROR CORRECTION UNIT
SERVICE PROVIDER MANAGEMENT UNIT
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
EMD SERVICE CENTER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
SAM MANAGEMENT UNIT
MEDIA SAM MANAGEMENT UNIT
STACK MEMORY
EXTERNAL MEMORY MANAGEMENT UNIT
SECURE CONTAINER DECRYPTION UNIT
USAGE MONITOR UNIT
ENCRYPTION-DECRYPTION UNIT(KSES)
ENCRYPTION-DECRYPTION UNIT (KSTR)
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
SIGNATURE PROCESSING UNIT
STORAGE UNIT
CHARGE PROCESSING UNIT
MUTUAL CERTIFICATION UNIT
304
181
580
184
185
190
197
200
811
182
312 PRICE TAG DATA
903
KD1~KD3 SIGKD1, ESC ~SIGKD3, ESC
CERSP
KF
CERCP, CERCP
186
KD1~KD3
171
172
173
183
589
192
587
170

FIG.77

STORED DATA OF STACK MEMORY 200

CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA(UCP) 106
LOCK KEY DATA K_{LOC} OF NOVOLATILE MEMORY 201
PUBLIC KEY CERTIFICATE DATA CER_{CP} OF CONTENT PROVIDER 301
PUBLIC KEY CERTIFICATE DATA CER_{SP} OF SERVICE PROVIDER 301
USAGE CONTROL STATUS DATA(UCS) 166
SAM PROGRAM DOWNLOAD CONTAINERS $SD_1 \sim SDC_3$
PRICE TAG DATA 312

FIG.78

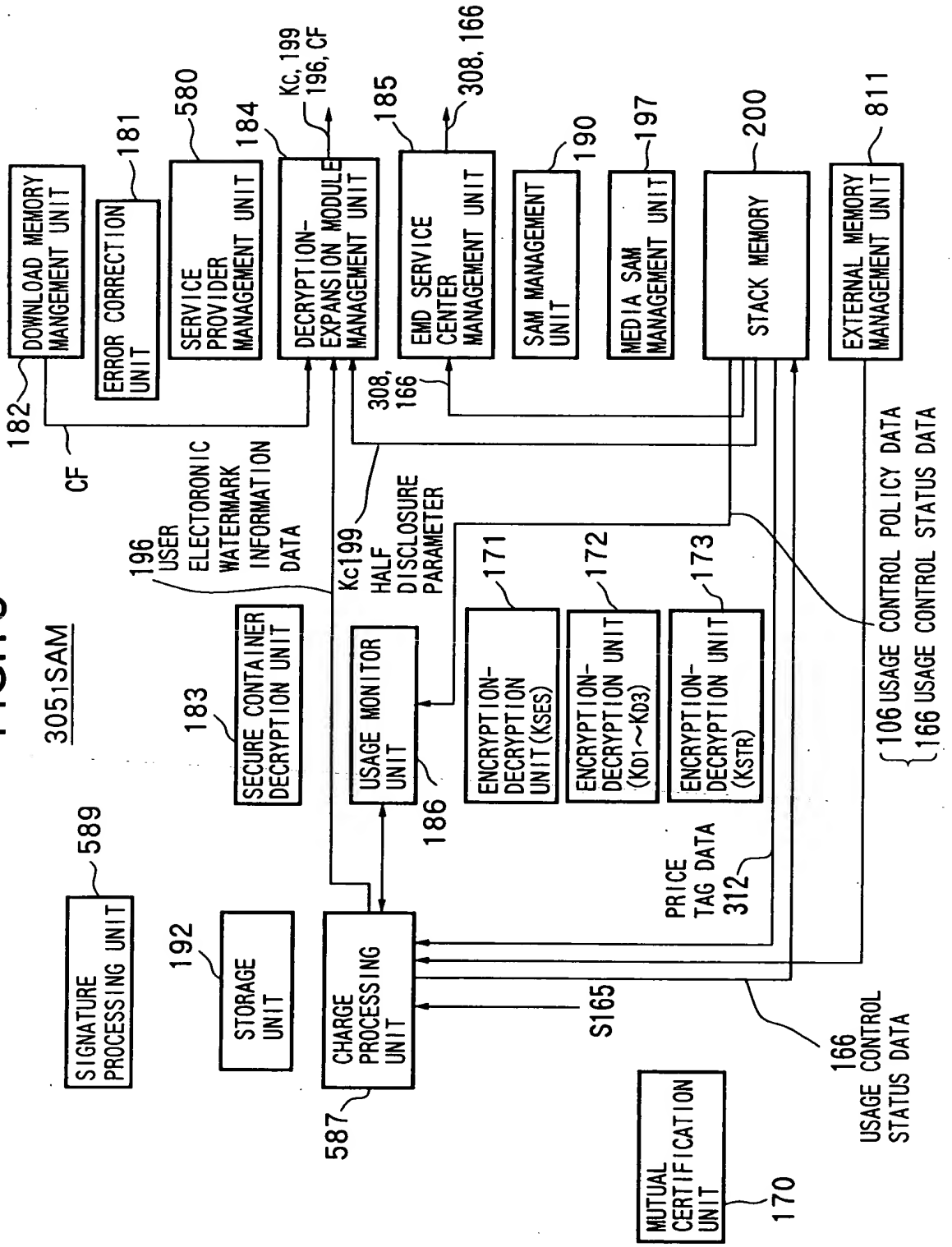

3051SAM
DOWNLOAD MEMORY MANGEMENT UNIT
182
CF
ERROR CORRECTION UNIT
181
SERVICE PROVIDER MANAGEMENT UNIT
580
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
Kc, 199
196, CF
EMD SERVICE CENTER MANAGEMENT UNIT
185
308, 166
SAM MANAGEMENT UNIT
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811
308, 166
196 USER ELECTORONIC WATERMARK INFORMATION DATA
Kc199 HALF DISCLOSURE PARAMETER
106 USAGE CONTROL POLICY DATA
166 USAGE CONTROL STATUS DATA
SECURE CONTAINER DECRYPTION UNIT
183
USAGE MONITOR UNIT
186
ENCRYPTION-DECRYPTION UNIT(KSES)
171
ENCRYPTION-DECRYPTION UNIT (KD1~KD3)
172
ENCRYPTION-DECRYPTION UNIT (KSTR)
173
PRICE TAG DATA
312
SIGNATURE PROCESSING UNIT
589
STORAGE UNIT
192
CHARGE PROCESSING UNIT
587
S165
166 USAGE CONTROL STATUS DATA
MUTUAL CERTIFICATION UNIT
170

FIG.79

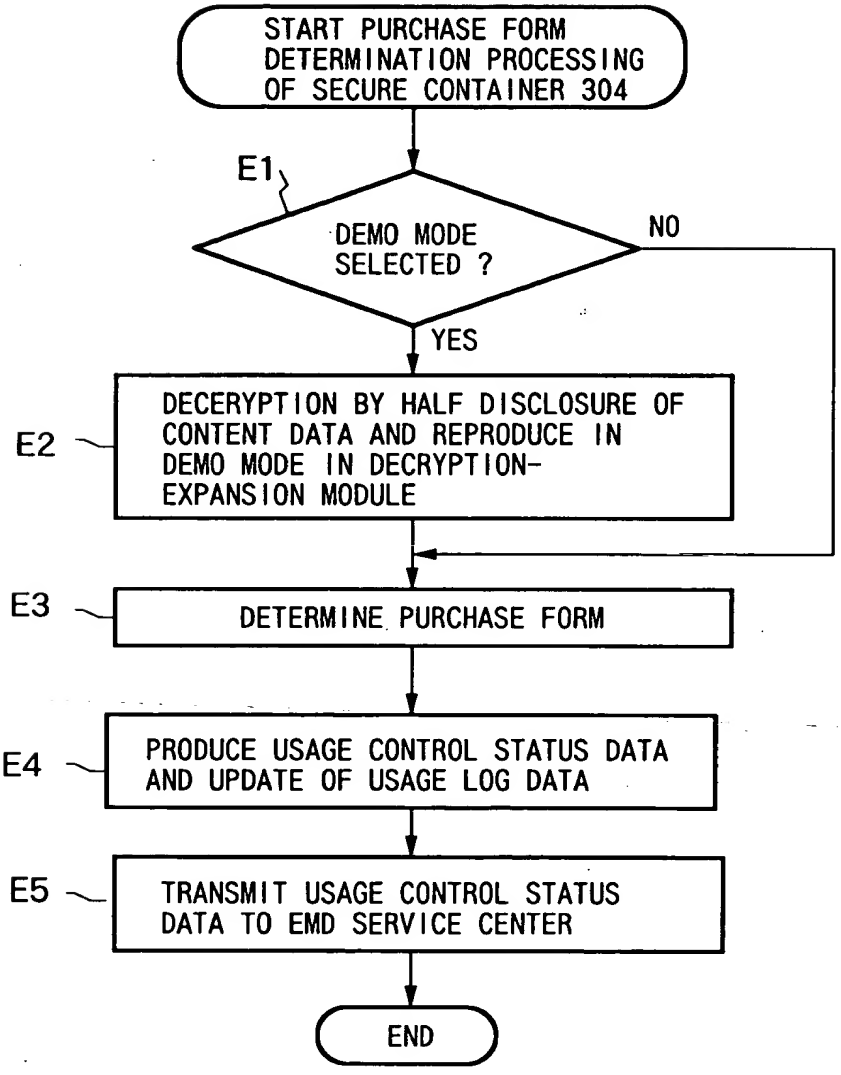

START PURCHASE FORM DETERMINATION PROCESSING OF SECURE CONTAINER 304
E1
DEMO MODE SELECTED ?
NO
YES
E2
DECERYPTION BY HALF DISCLOSURE OF CONTENT DATA AND REPRODUCE IN DEMO MODE IN DECRYPTION-EXPANSION MODULE
E3
DETERMINE PURCHASE FORM
E4
PRODUCE USAGE CONTROL STATUS DATA AND UPDATE OF USAGE LOG DATA
E5
TRANSMIT USAGE CONTROL STATUS DATA TO EMD SERVICE CENTER
END

FIG.80

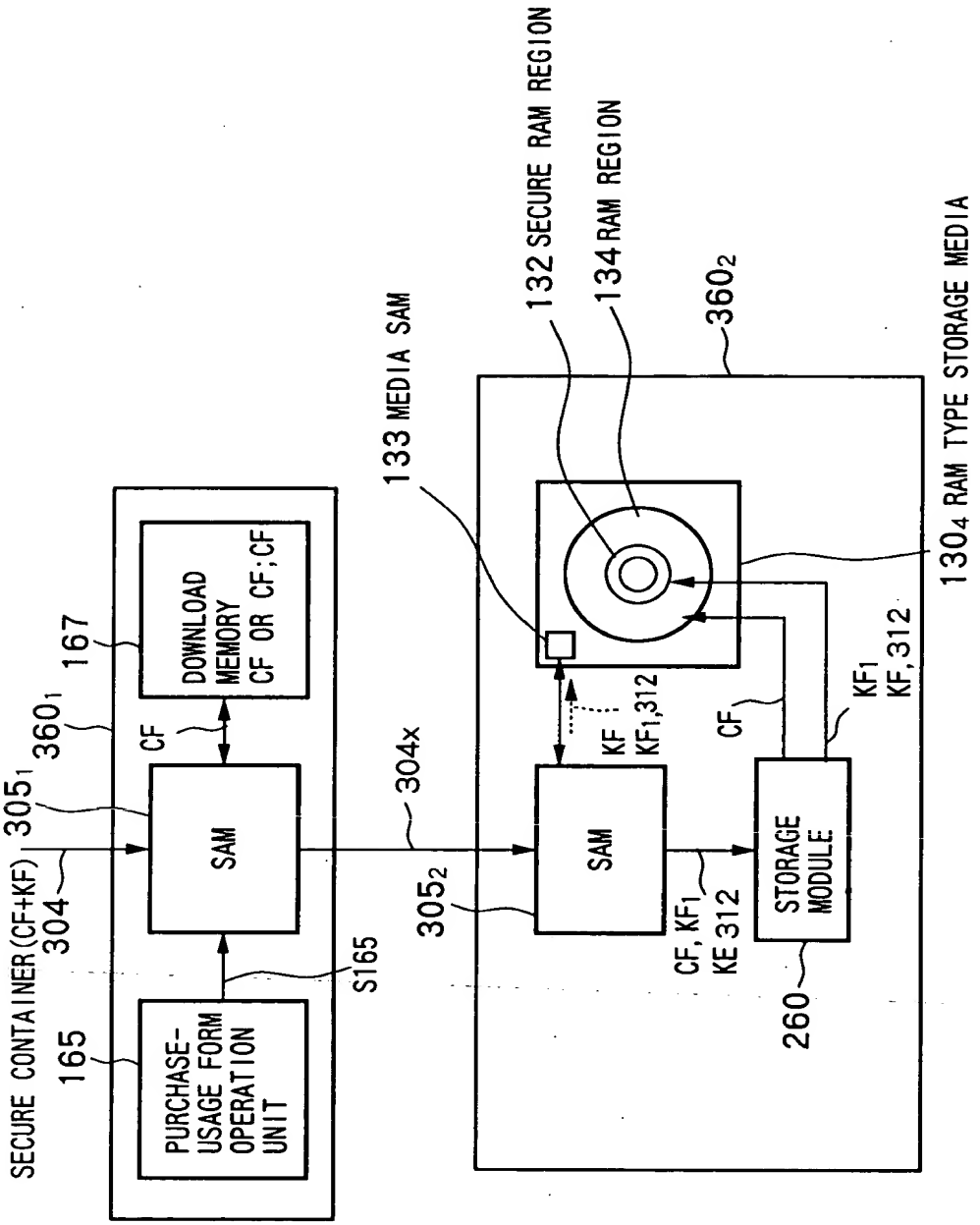


FIG.81A

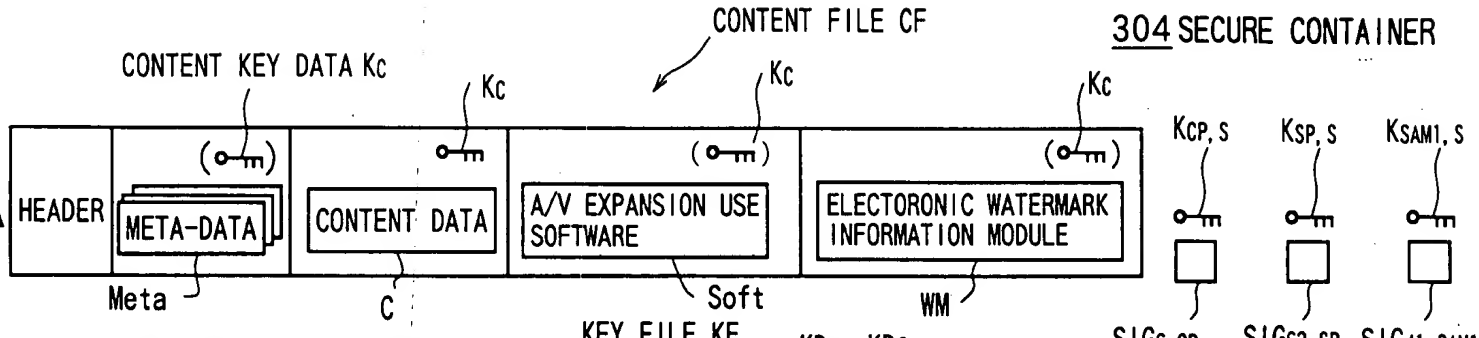


FIG.81B

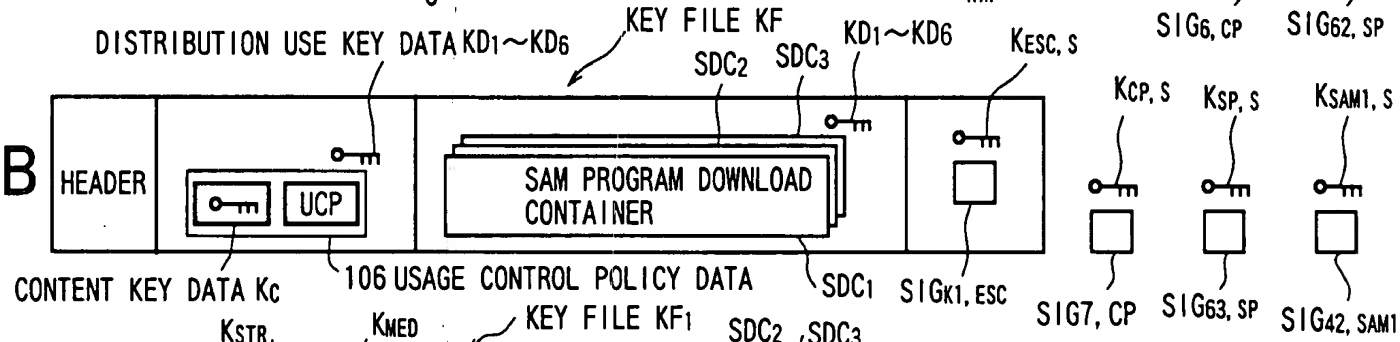


FIG.81C

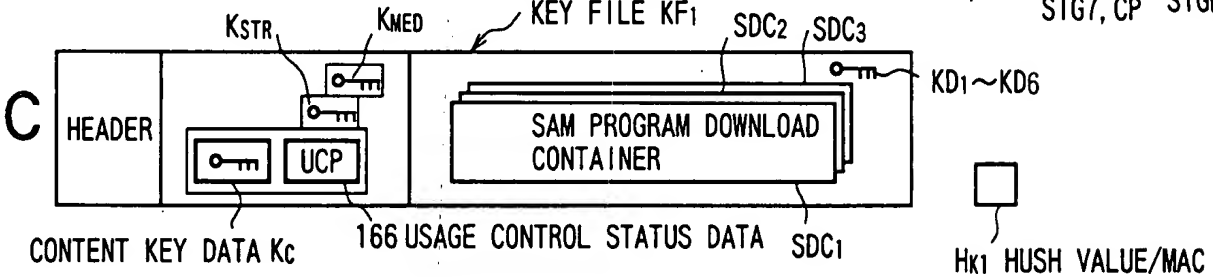


FIG.81D

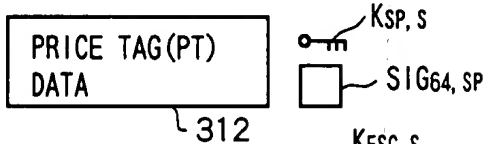


FIG.81E

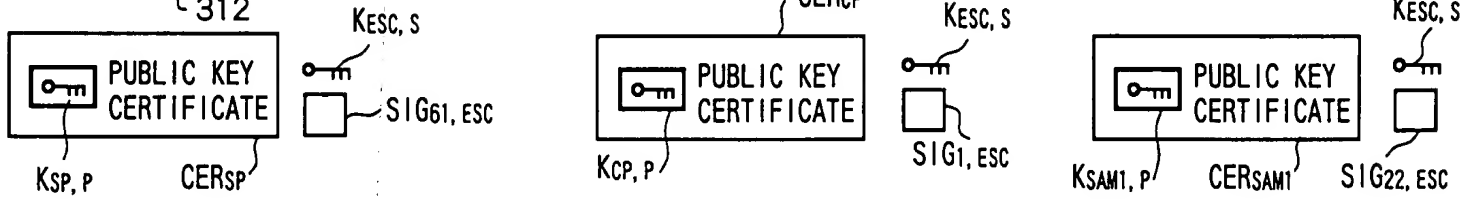


FIG.82

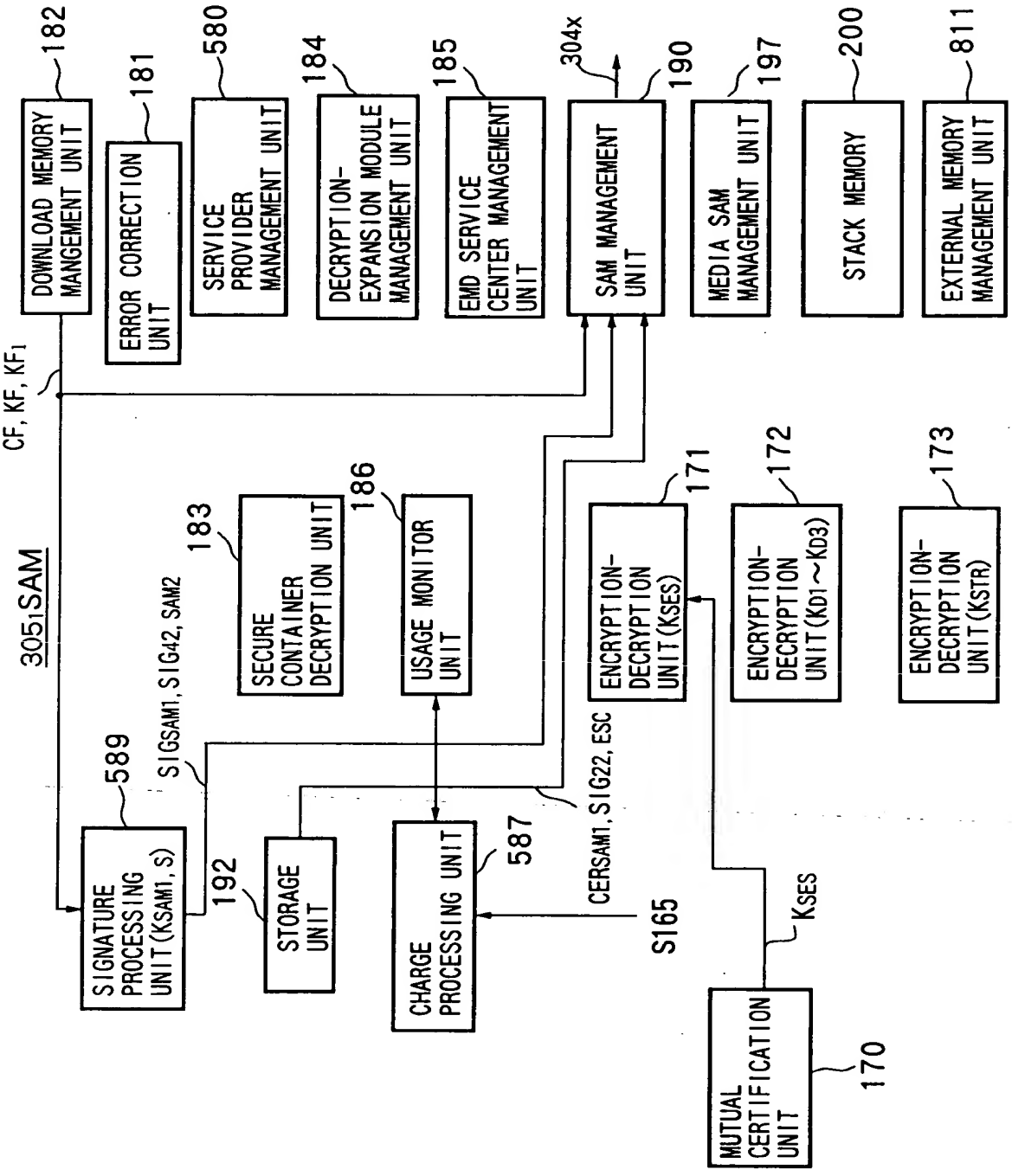

305 SAM
DOWNLOAD MEMORY MANGEMENT UNIT
182
ERROR CORRECTION UNIT
181
SERVICE PROVIDER MANAGEMENT UNIT
580
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
SAM MANAGEMENT UNIT
304x
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGEMENT UNIT
811
CF, KF, KF1
SECURE CONTAINER DECRYPTION UNIT
183
USAGE MONITOR UNIT
186
ENCRYPTION-DECRYPTION UNIT(KSES)
171
ENCRYPTION-DECRYPTION UNIT(KD1~KD3)
172
ENCRYPTION-DECRYPTION UNIT(KSTR)
173
SIGSAM1, SIG42, SAM2
589
SIGNATURE PROCESSING UNIT(KSAM1, S)
192
STORAGE UNIT
CHARGE PROCESSING UNIT
587
CERSAM1, SIG22, ESC
S165
KSES
MUTUAL CERTIFICATION UNIT
170

FIG.83

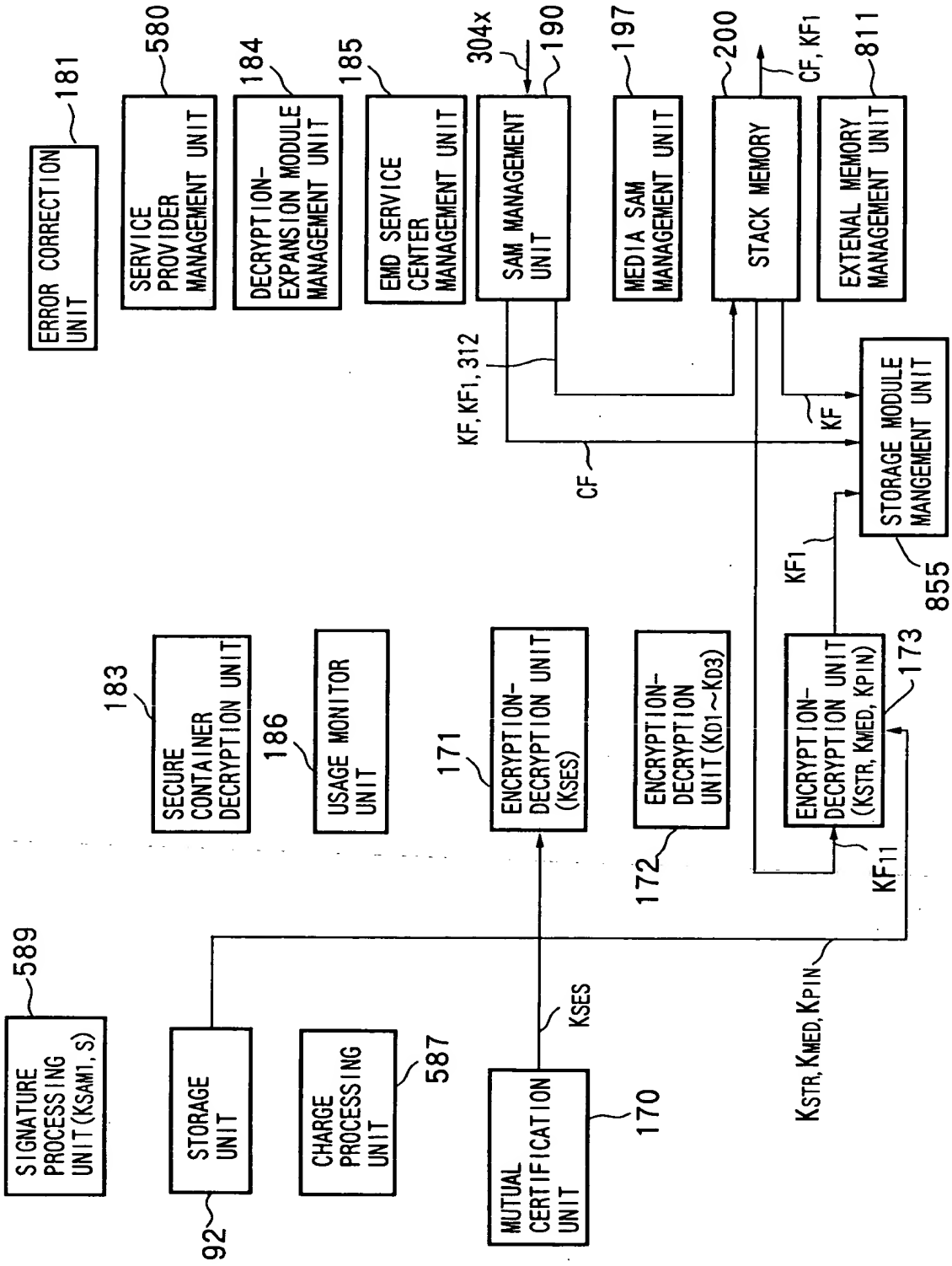

305₂SAM
ERROR CORRECTION UNIT
181
SERVICE PROVIDER MANAGEMENT UNIT
580
DECRYPTION-EXPANSION MODULE MANAGEMENT UNIT
184
EMD SERVICE CENTER MANAGEMENT UNIT
185
304x
SAM MANAGEMENT UNIT
190
MEDIA SAM MANAGEMENT UNIT
197
STACK MEMORY
200
CF, KF1
EXTENAL MEMORY MANAGEMENT UNIT
811
KF, KF1, 312
CF
KF
STORAGE MODULE MANGEMENT UNIT
855
KF1
183
SECURE CONTAINER DECRYPTION UNIT
186
USAGE MONITOR UNIT
171
ENCRYPTION-DECRYPTION UNIT (KSES)
ENCRYPTION-DECRYPTION UNIT (KD1~KD3)
172
ENCRYPTION-DECRYPTION UNIT (KSTR, KMED, KPIN)
173
KF11
589
SIGNATURE PROCESSING UNIT (KSAM1, S)
STORAGE UNIT
192
CHARGE PROCESSING UNIT
587
MUTUAL CERTIFICATION UNIT
170
KSES
KSTR, KMED, KPIN

FIG.84

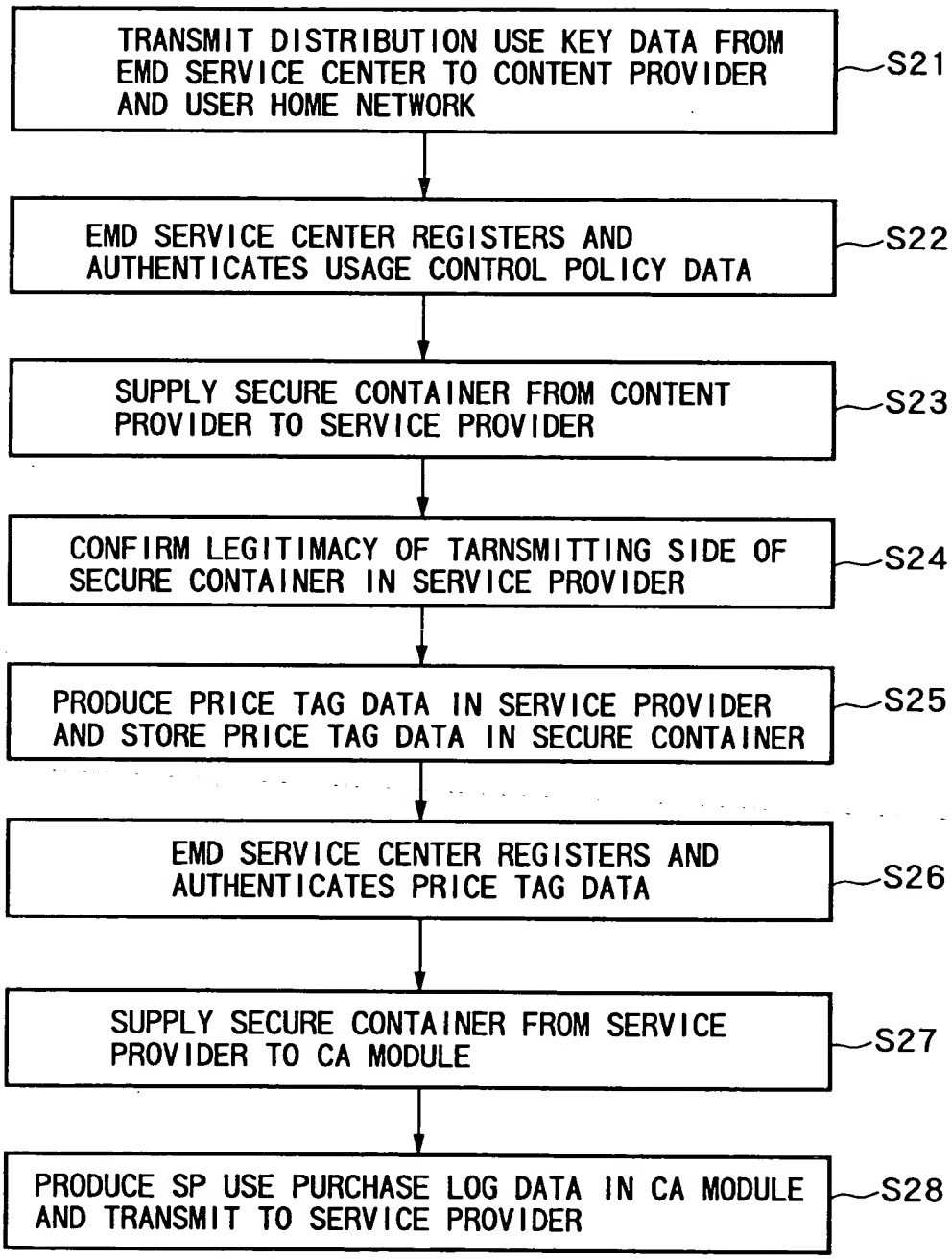


FIG.85

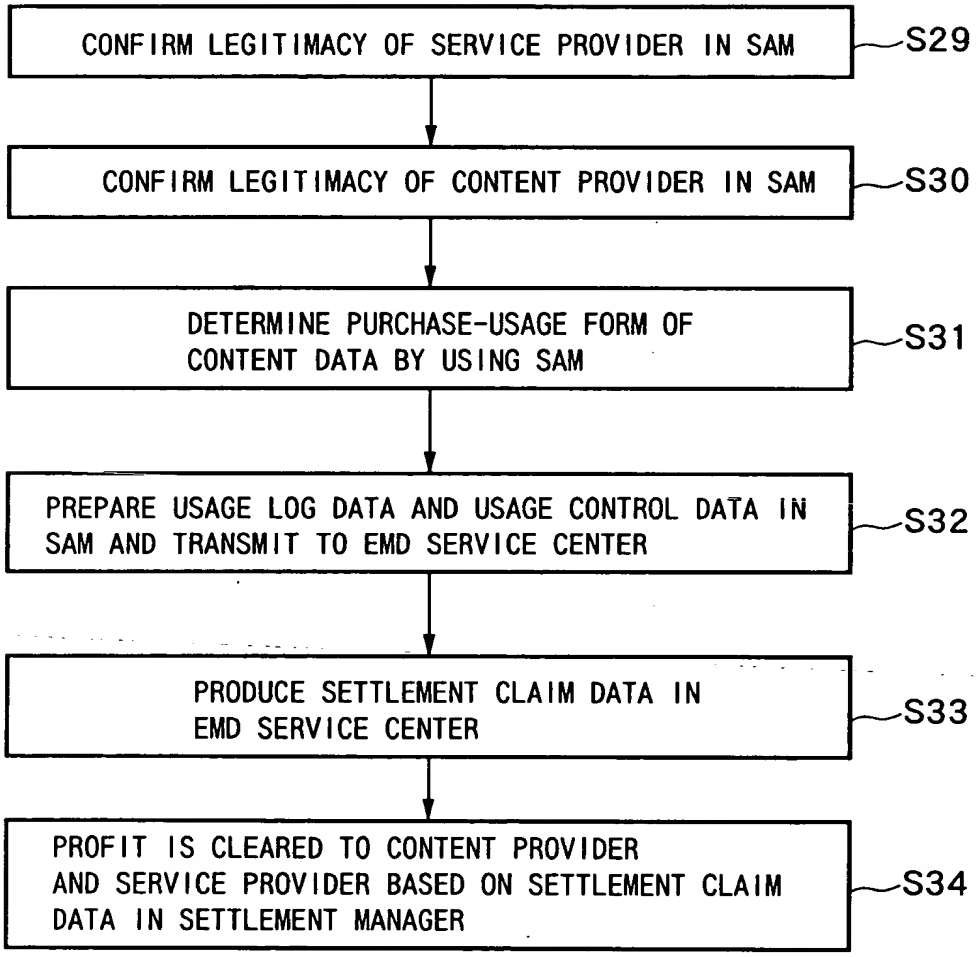


FIG.86

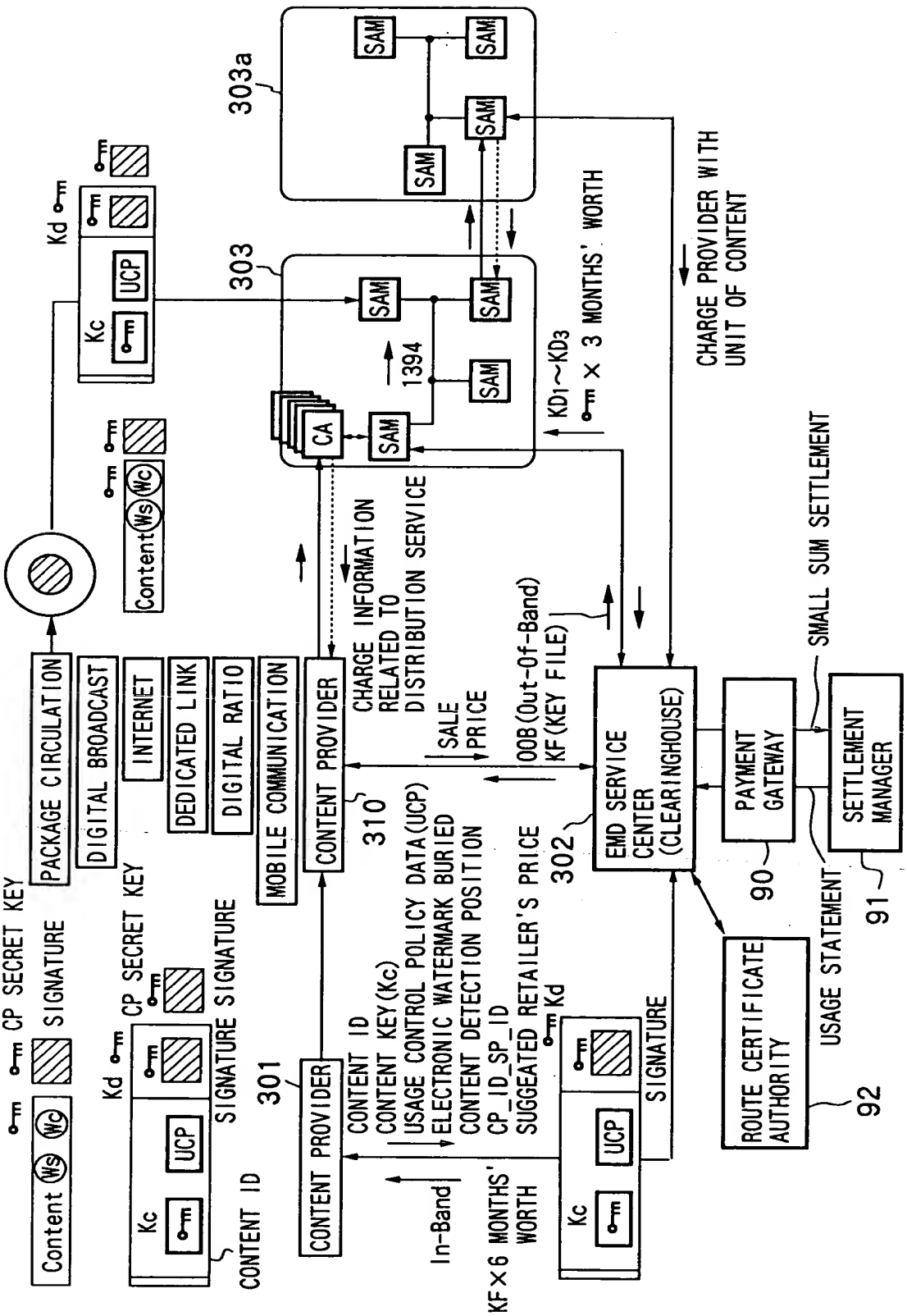

303a
SAM
303
CA
1394
KD1~KD3
× 3 MONTHS' WORTH
CHARGE PROVIDER WITH UNIT OF CONTENT
Kd
Kc
UCP
Content
Ws
Wc
PACKAGE CIRCULATION
DIGITAL BROADCAST
INTERNET
DEDICATED LINK
DIGITAL RATIO
MOBILE COMMUNICATION
CP SECRET KEY
SIGNATURE
CONTENT ID
301
CONTENT PROVIDER
310
CHARGE INFORMATION RELATED TO DISTRIBUTION SERVICE
SALE PRICE
OOB(Out-Of-Band)
KF(KEY FILE)
CONTENT ID
CONTENT KEY(Kc)
USAGE CONTROL POLICY DATA(UCP)
ELECTRONIC WATERMARK BURIED
CONTENT DETECTION POSITION
CP_ID_SP_ID
SUGGEATED RETAILER'S PRICE
In-Band
KF×6 MONTHS' WORTH
EMD SERVICE CENTER (CLEARINGHOUSE)
302
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
SMALL SUM SETTLEMENT
ROUTE CERTIFICATE AUTHORITY
92
USAGE STATEMENT

FIG.87

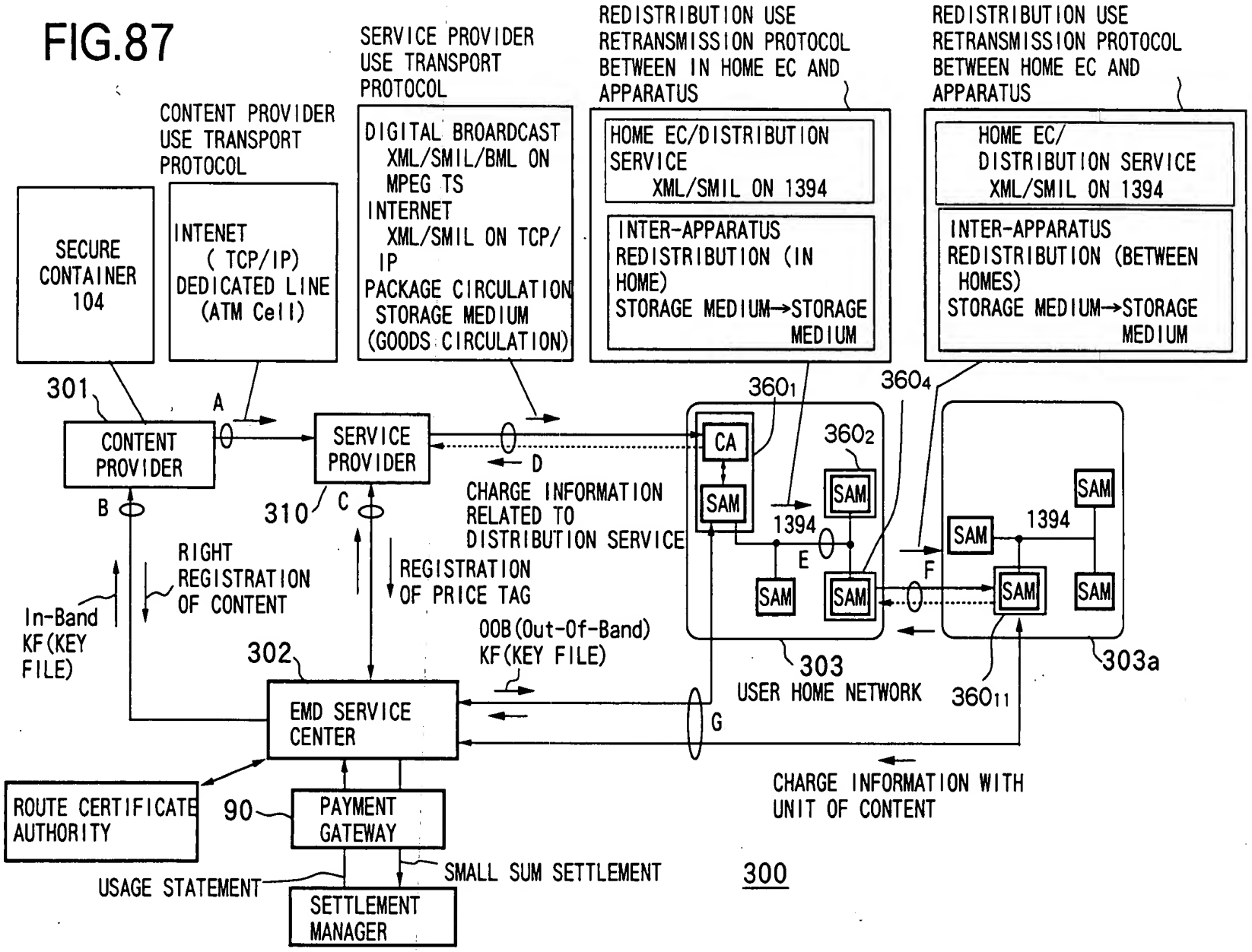


FIG.88

CONTENT PROVIDER
SERVICE PROVIDER
CONTENT PROVIDER 301
CONTENT PROVIDER SECURE CONTAINER USE COMMODITY TRANSPORT PROTOCOL
SERVICE PROVIDER310
CONTENT PROVIDER SECURE CONTAINER USE COMMODITY TRANSPORT PROTOCOL
Application
XML/SMIL
http/s-http
SSL
TCP
UDP
IP/IP-SEC
MAC
PHY
XDR
RPC
Control
CP USE SECURE CONTAINER DATABESE 118a
SP USE SECURE CONTAINER DATABESE 355a
KF
CF
PT
TRUE RANDOM NUMBER
CP B SECRET KEY
SP C PUBLIC KEY
PUBLIC KEY ENCRYPTION MUTUAL CERTIFICATION
(KEY IS SHARED)
COMMON KEY (SESSION KEY)
SIGNATURE VERIFICATION
TRUE RANDOM NUMBER
SP C SECRET KEY
CP B PUBLIC KEY
MUTUAL CERTIFICATION BY PUBLIC KEY METHOD
(KEY IS SHARED)
COMMON KEY (SESSION KEY)
SIGNATURE VERIFICATION
104 SECURE CONTAINER

FIG.89

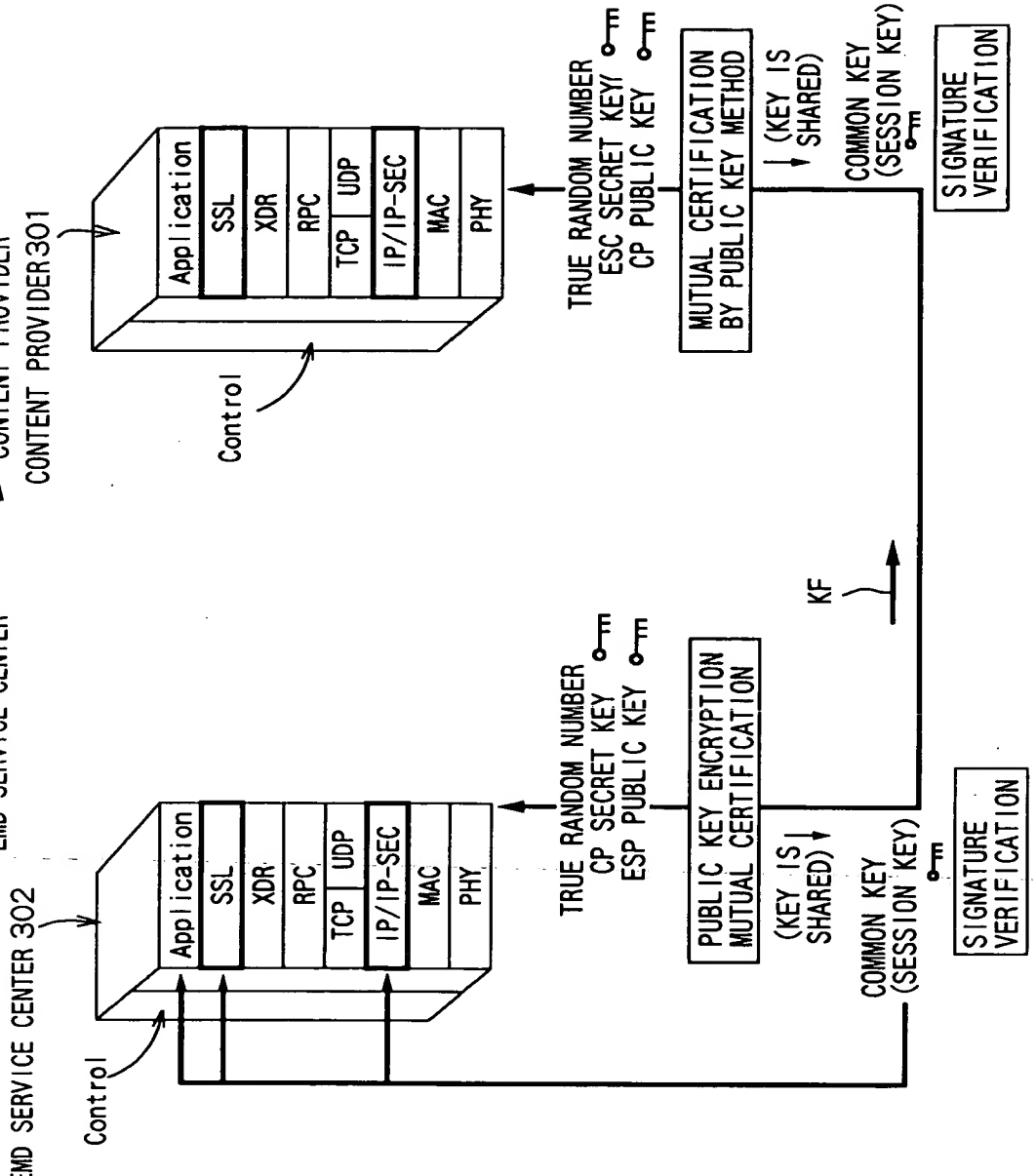


FIG.90

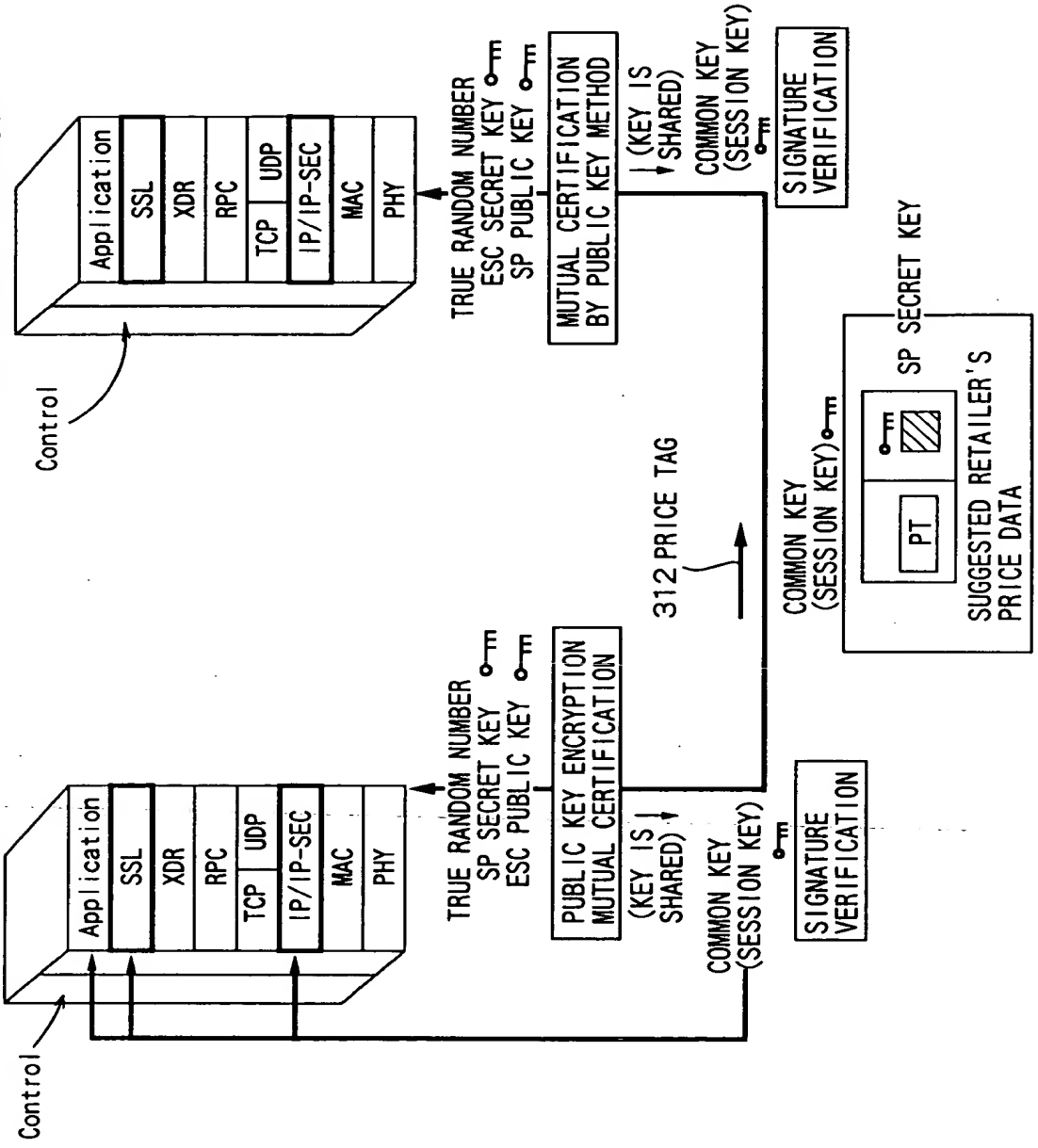

SERVICE PROVIDER
EMD SERVICE CENTER
SERVICE PROVIDER 310
EMD SERVICE CENTER 302
Application
SSL
XDR
RPC
TCP
UDP
IP/IP-SEC
MAC
PHY
Control
TRUE RANDOM NUMBER
SP SECRET KEY
ESC PUBLIC KEY
PUBLIC KEY ENCRYPTION MUTUAL CERTIFICATION
MUTUAL CERTIFICATION BY PUBLIC KEY METHOD
(KEY IS SHARED)
COMMON KEY (SESSION KEY)
SIGNATURE VERIFICATION
312 PRICE TAG
PT
SP SECRET KEY
SUGGESTED RETAILER'S PRICE DATA

FIG.91

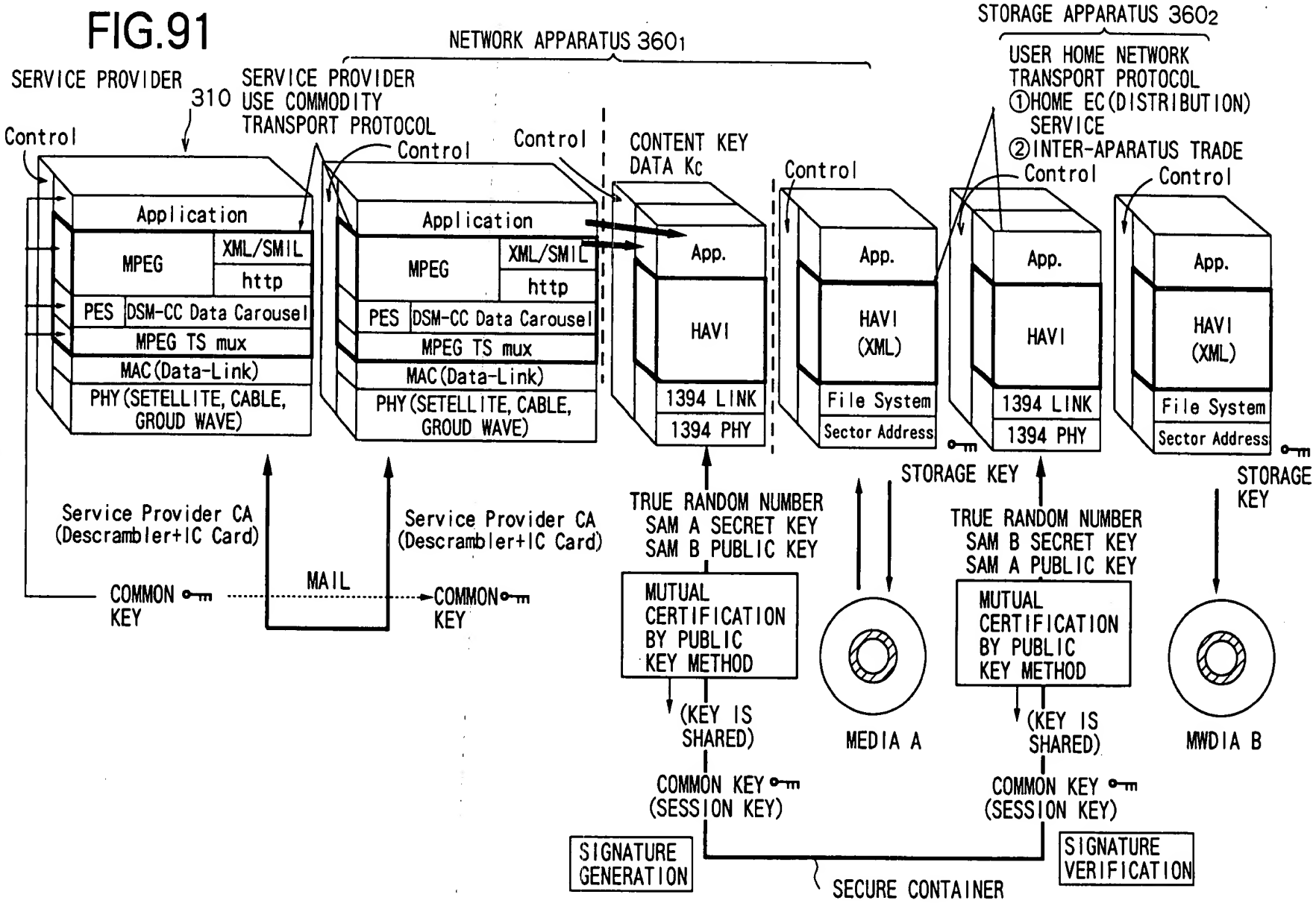

NETWORK APPARATUS 360₁
STORAGE APPARATUS 360₂
SERVICE PROVIDER
310
SERVICE PROVIDER USE COMMODITY TRANSPORT PROTOCOL
USER HOME NETWORK TRANSPORT PROTOCOL
①HOME EC(DISTRIBUTION) SERVICE
②INTER-APARATUS TRADE
Control
CONTENT KEY DATA Kc
Application
MPEG
XML/SMIL
http
PES
DSM-CC Data Carousel
MPEG TS mux
MAC(Data-Link)
PHY(SETELLITE, CABLE, GROUD WAVE)
App.
HAVI
HAVI (XML)
1394 LINK
1394 PHY
File System
Sector Address
Service Provider CA (Descrambler+IC Card)
MAIL
COMMON KEY
STORAGE KEY
TRUE RANDOM NUMBER
SAM A SECRET KEY
SAM B PUBLIC KEY
SAM B SECRET KEY
SAM A PUBLIC KEY
MUTUAL CERTIFICATION BY PUBLIC KEY METHOD
(KEY IS SHARED)
COMMON KEY (SESSION KEY)
MEDIA A
MWDIA B
SIGNATURE GENERATION
SIGNATURE VERIFICATION
SECURE CONTAINER

FIG.92

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE XML/SMIL/BML IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

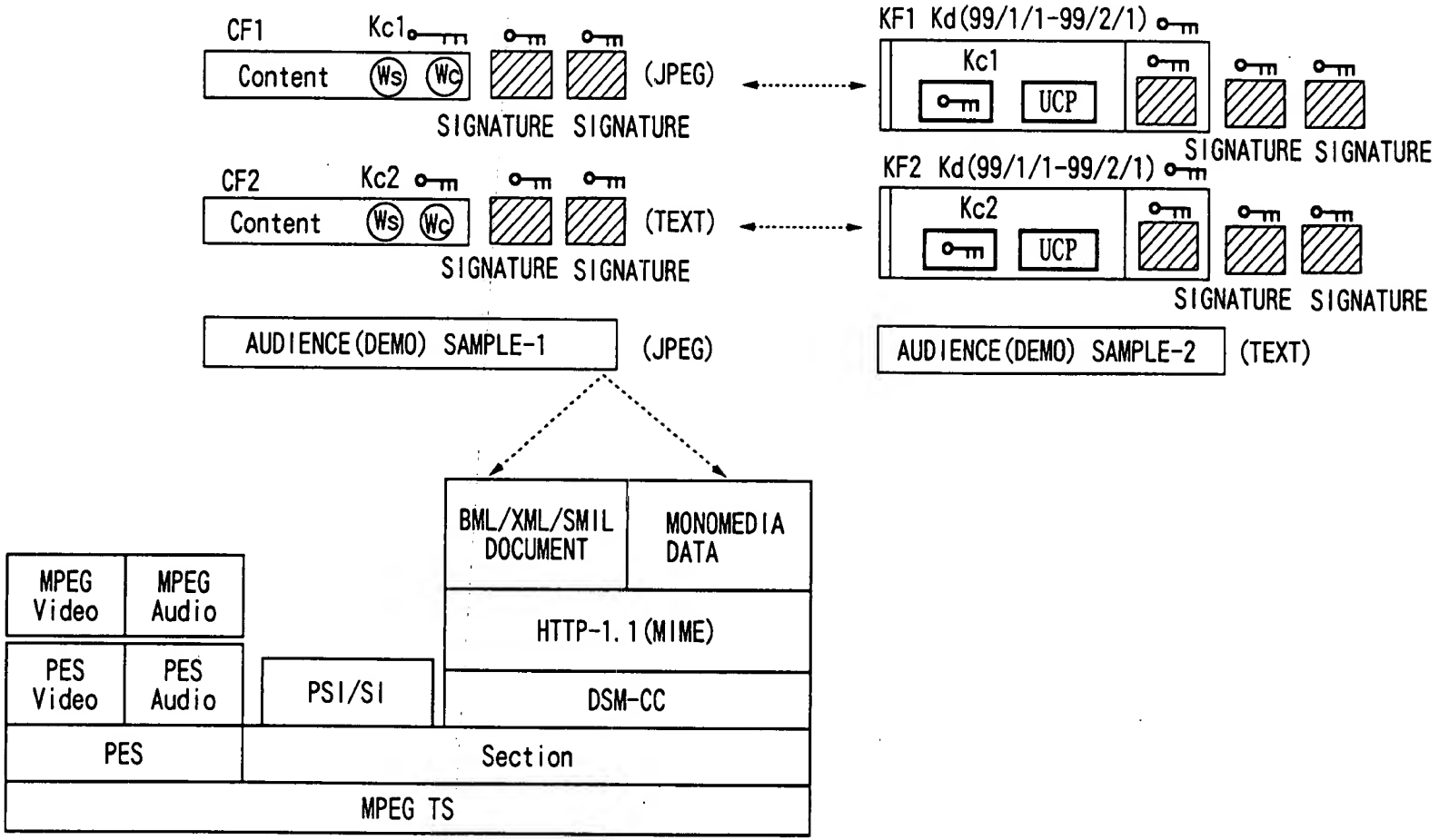


FIG.93

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE MHEG IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

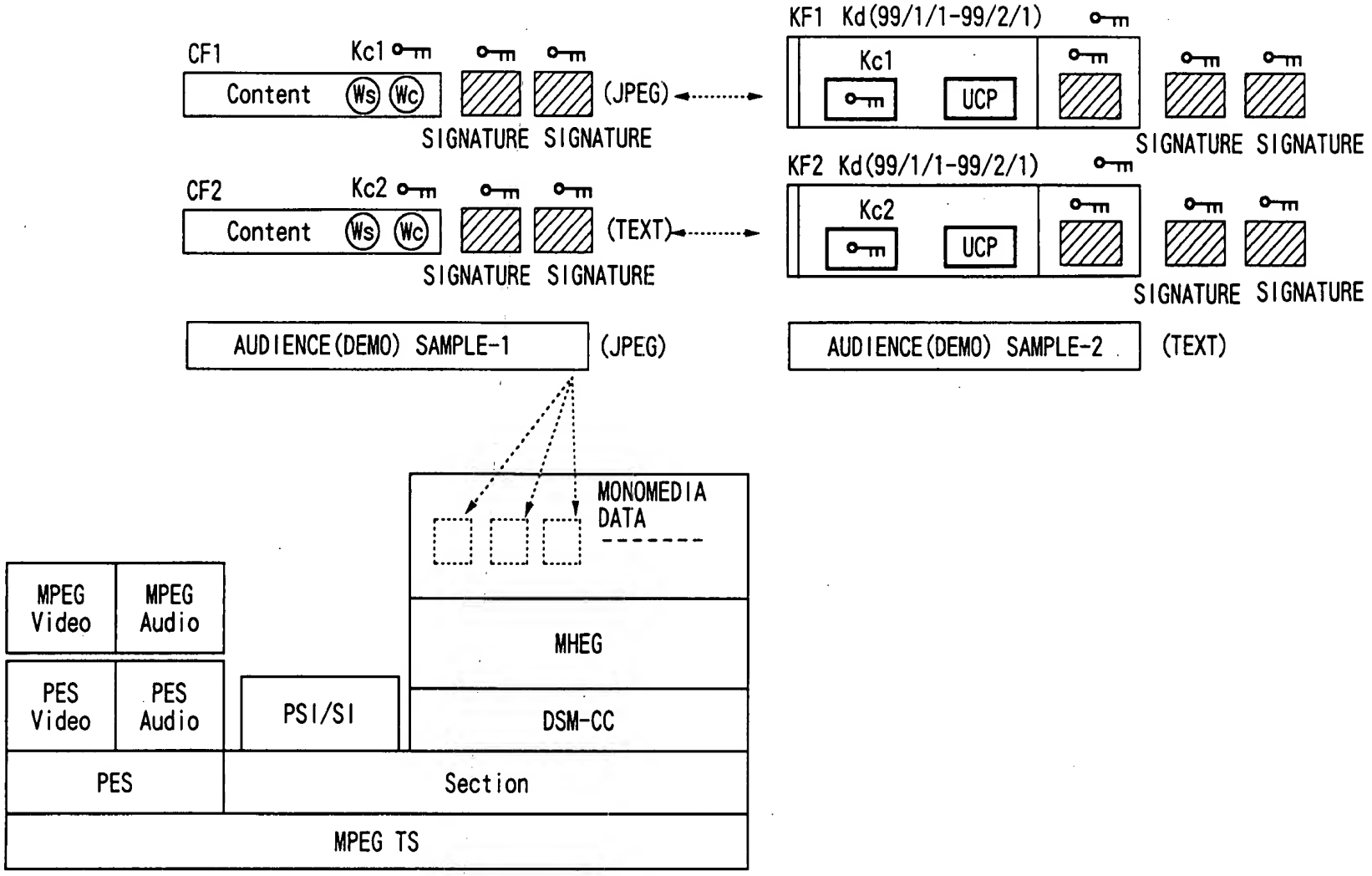


FIG.94

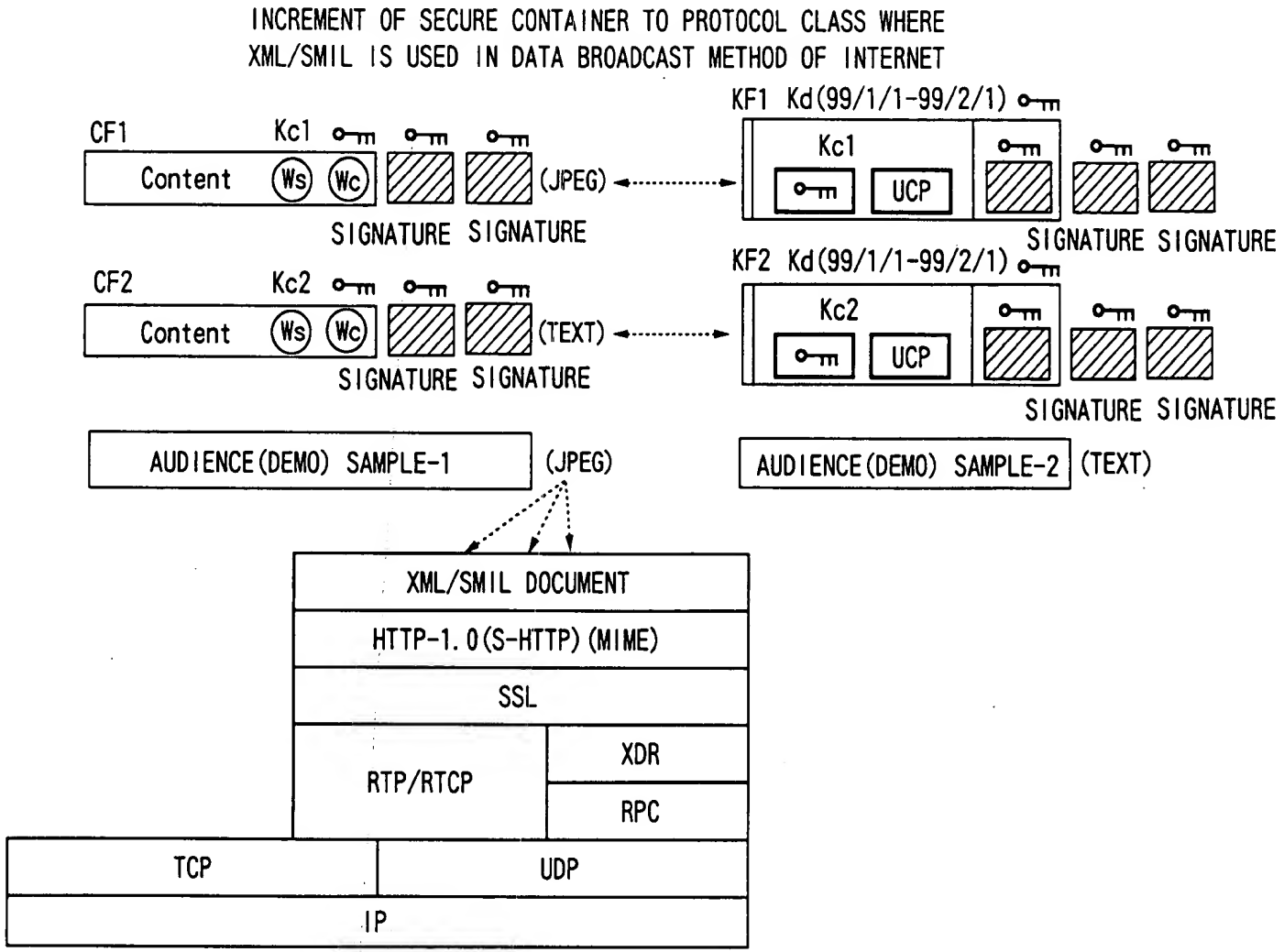


FIG.95

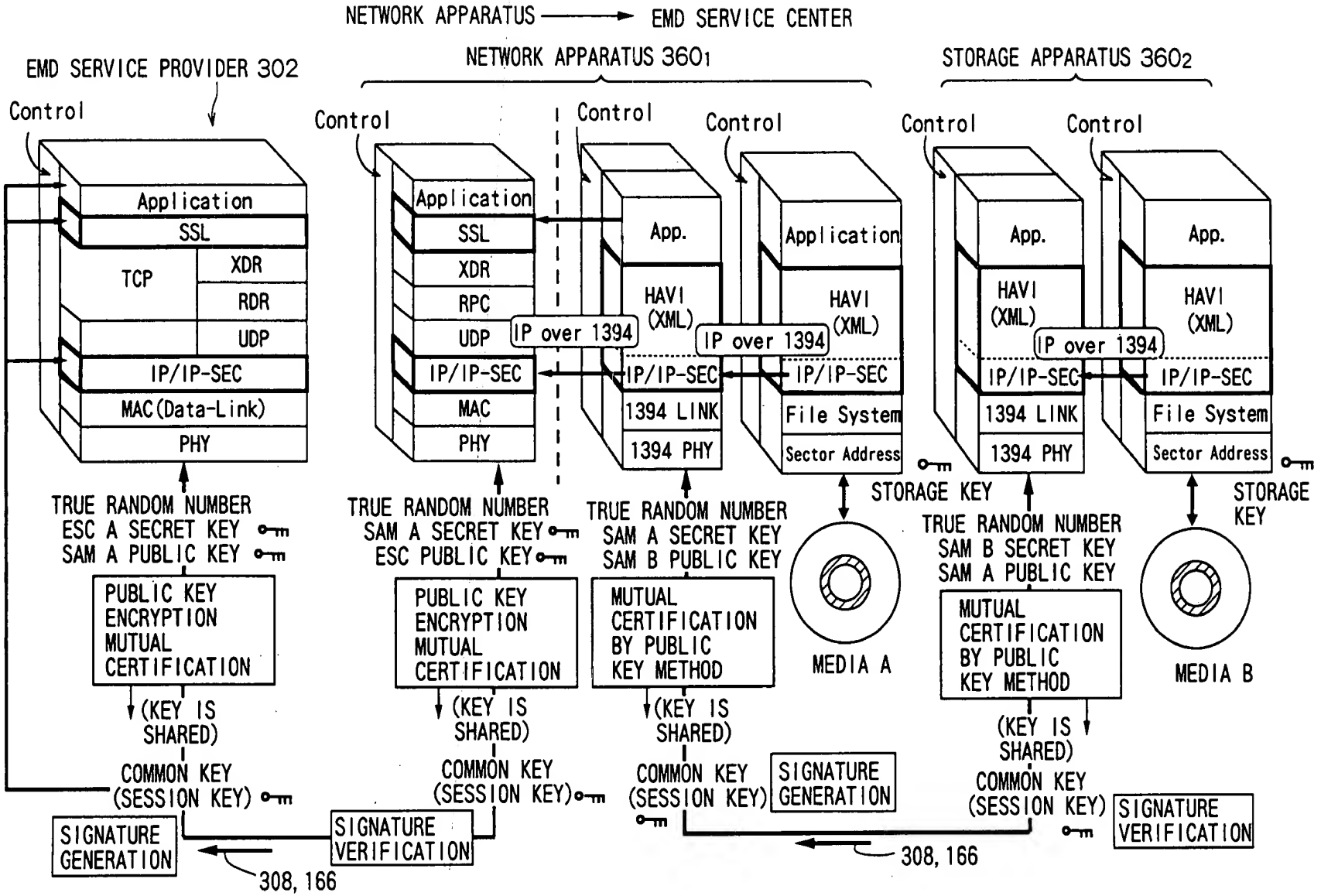

NETWORK APPARATUS → EMD SERVICE CENTER
EMD SERVICE PROVIDER 302
NETWORK APPARATUS 360₁
STORAGE APPARATUS 360₂
Control
Application
SSL
TCP
XDR
RDR
UDP
IP/IP-SEC
MAC(Data-Link)
PHY
RPC
MAC
App.
HAVI (XML)
IP over 1394
1394 LINK
1394 PHY
File System
Sector Address
TRUE RANDOM NUMBER
ESC A SECRET KEY
SAM A PUBLIC KEY
SAM A SECRET KEY
ESC PUBLIC KEY
SAM B SECRET KEY
PUBLIC KEY ENCRYPTION MUTUAL CERTIFICATION
MUTUAL CERTIFICATION BY PUBLIC KEY METHOD
(KEY IS SHARED)
COMMON KEY (SESSION KEY)
SIGNATURE GENERATION
SIGNATURE VERIFICATION
STORAGE KEY
MEDIA A
MEDIA B
308, 166

FIG.96

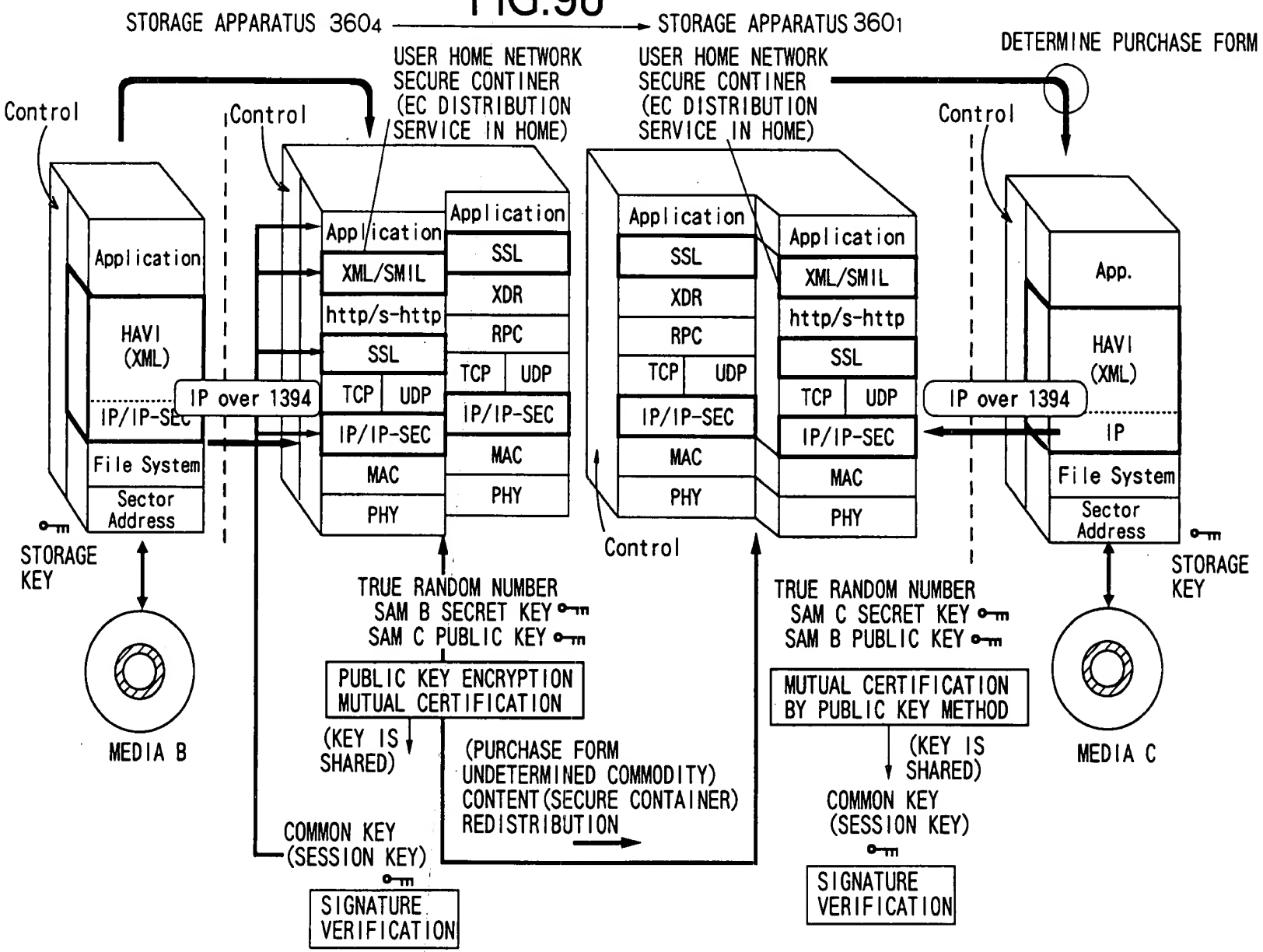


FIG.97

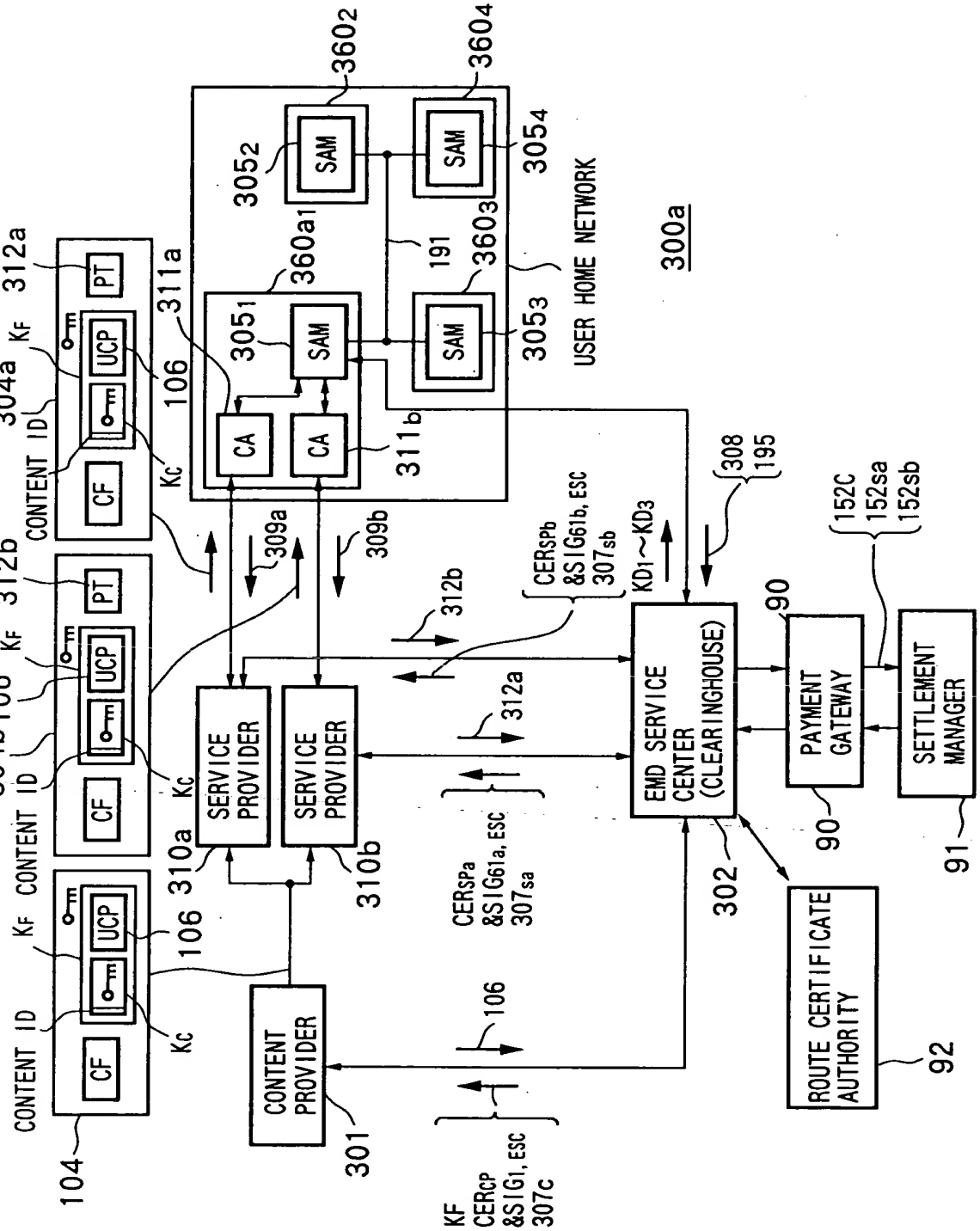

USER HOME NETWORK
300a
SAM
CA
PT
UCP
CF
CONTENT ID
SERVICE PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
ROUTE CERTIFICATE AUTHORITY
Kc
KF
106
191
195
302
301
104
90
91
92

FIG.98

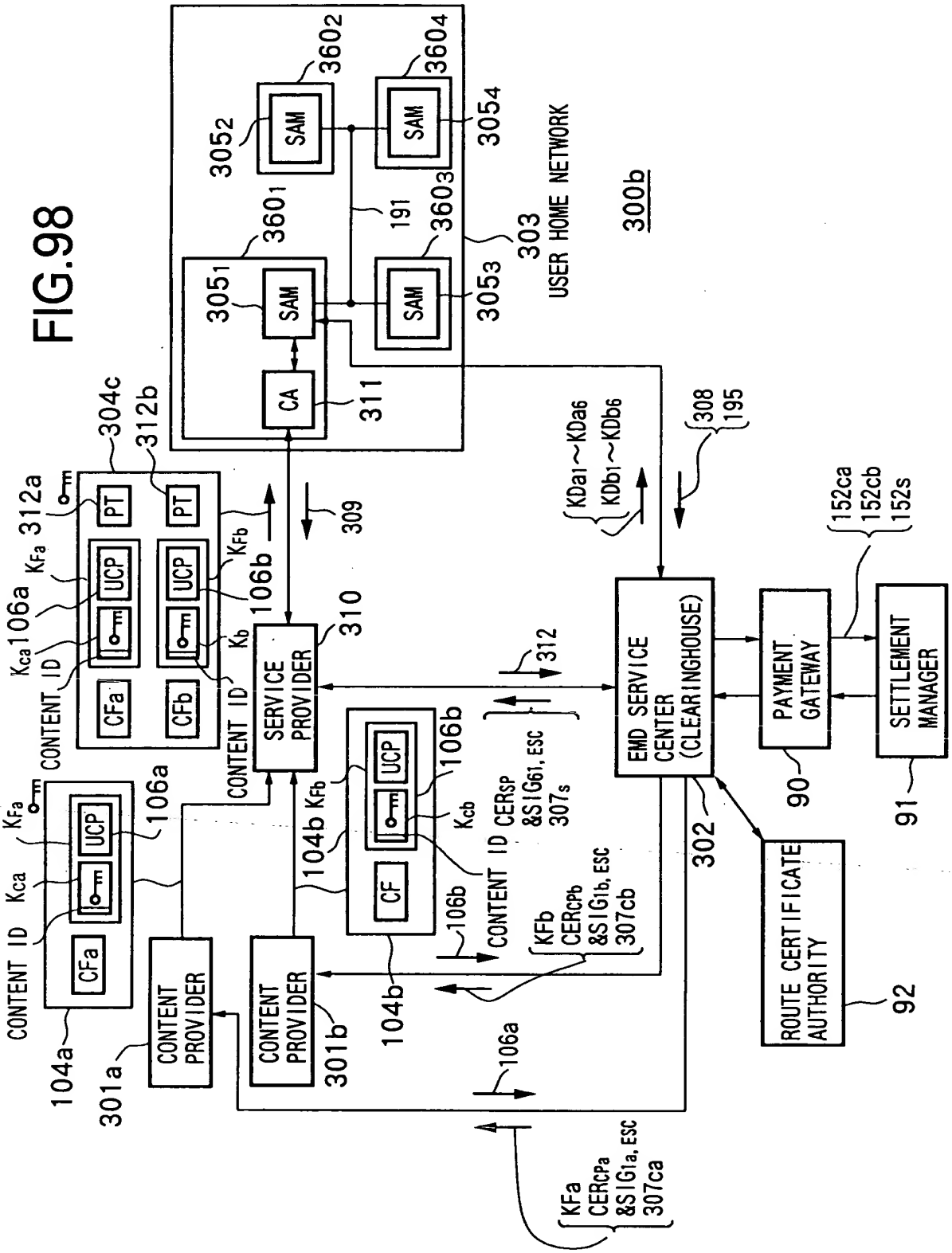

300b
USER HOME NETWORK
303
SAM
CA
PT
UCP
CF
CFa
CFb
SERVICE PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
ROUTE CERTIFICATE AUTHORITY
CONTENT ID
KDa1~KDa6
KDb1~KDb6
KFa CERCPa &SIG1a, ESC 307ca
KFb CERCPb &SIG1b, ESC 307cb
CONTENT ID CERSP &SIG61, ESC 307s

FIG.99

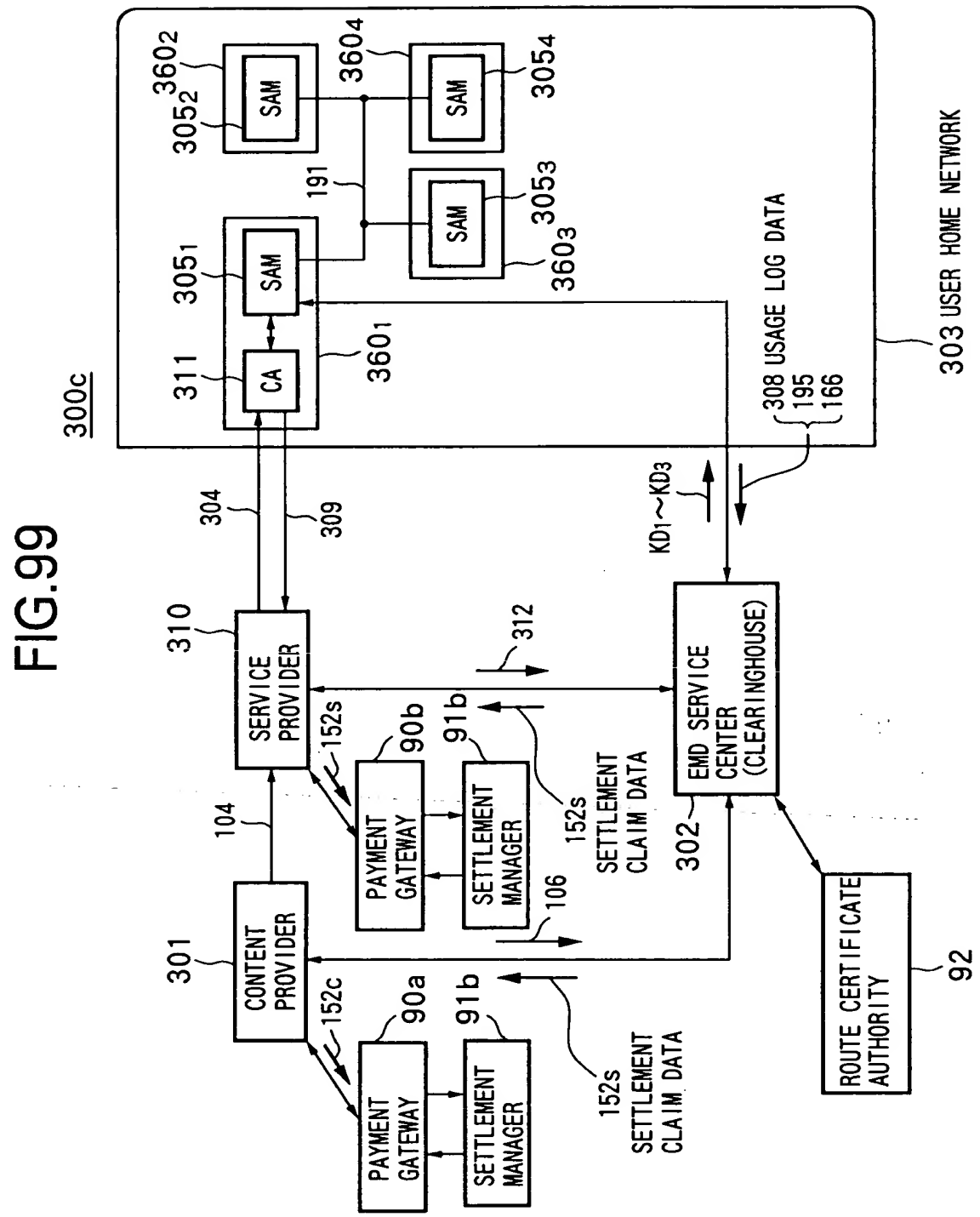

300c
SAM
CA
3602
3604
3054
3052
3053
3051
3603
3601
191
311
308 USAGE LOG DATA
195
166
303 USER HOME NETWORK
KD1~KD3
304
309
310
SERVICE PROVIDER
312
152s
90b
91b
PAYMENT GATEWAY
SETTLEMENT MANAGER
152s SETTLEMENT CLAIM DATA
EMD SERVICE CENTER (CLEARINGHOUSE)
104
106
302
301
CONTENT PROVIDER
152c
90a
91b
PAYMENT GATEWAY
SETTLEMENT MANAGER
152s SETTLEMENT CLAIM DATA
ROUTE CERTIFICATE AUTHORITY
92

FIG.100

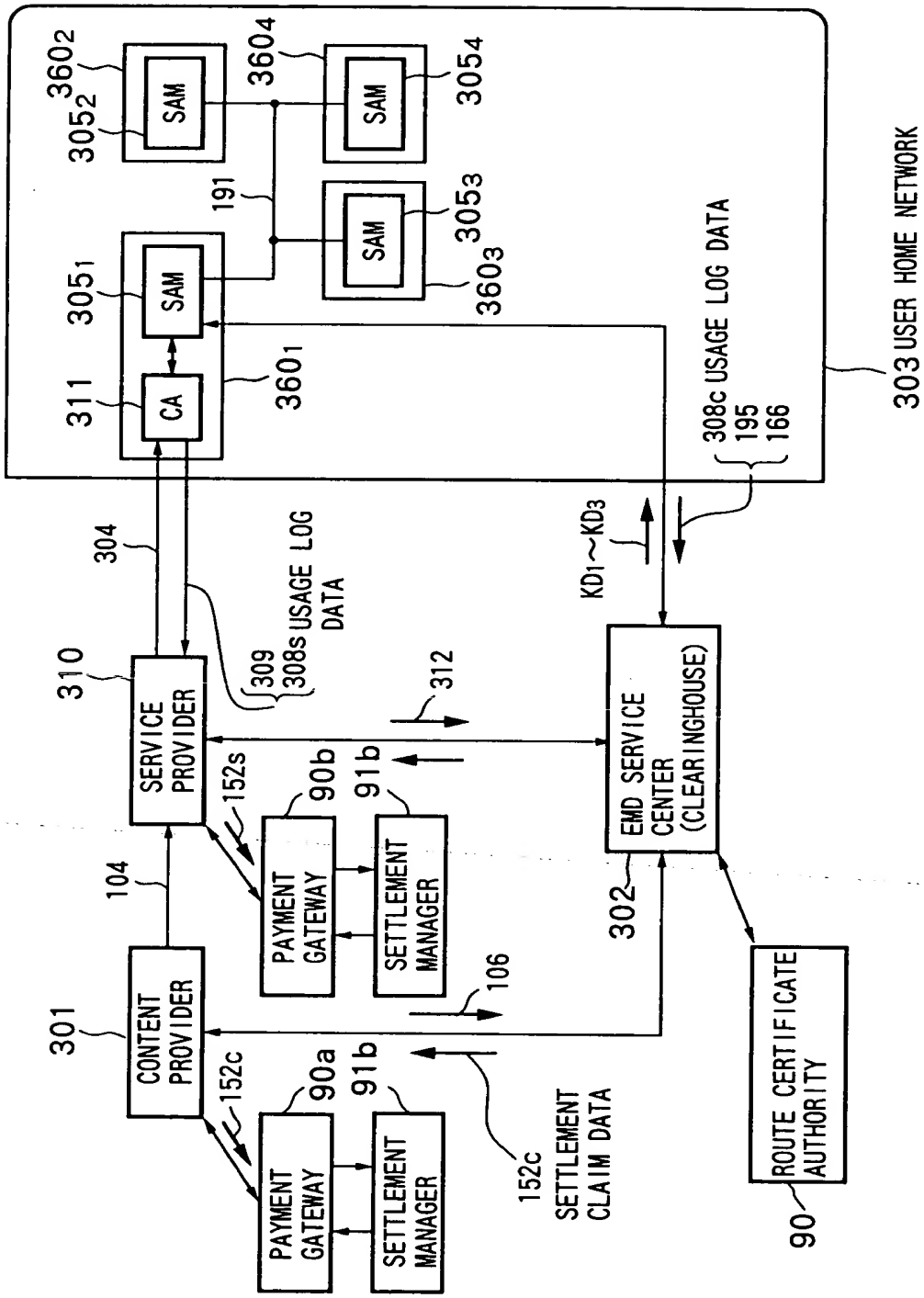
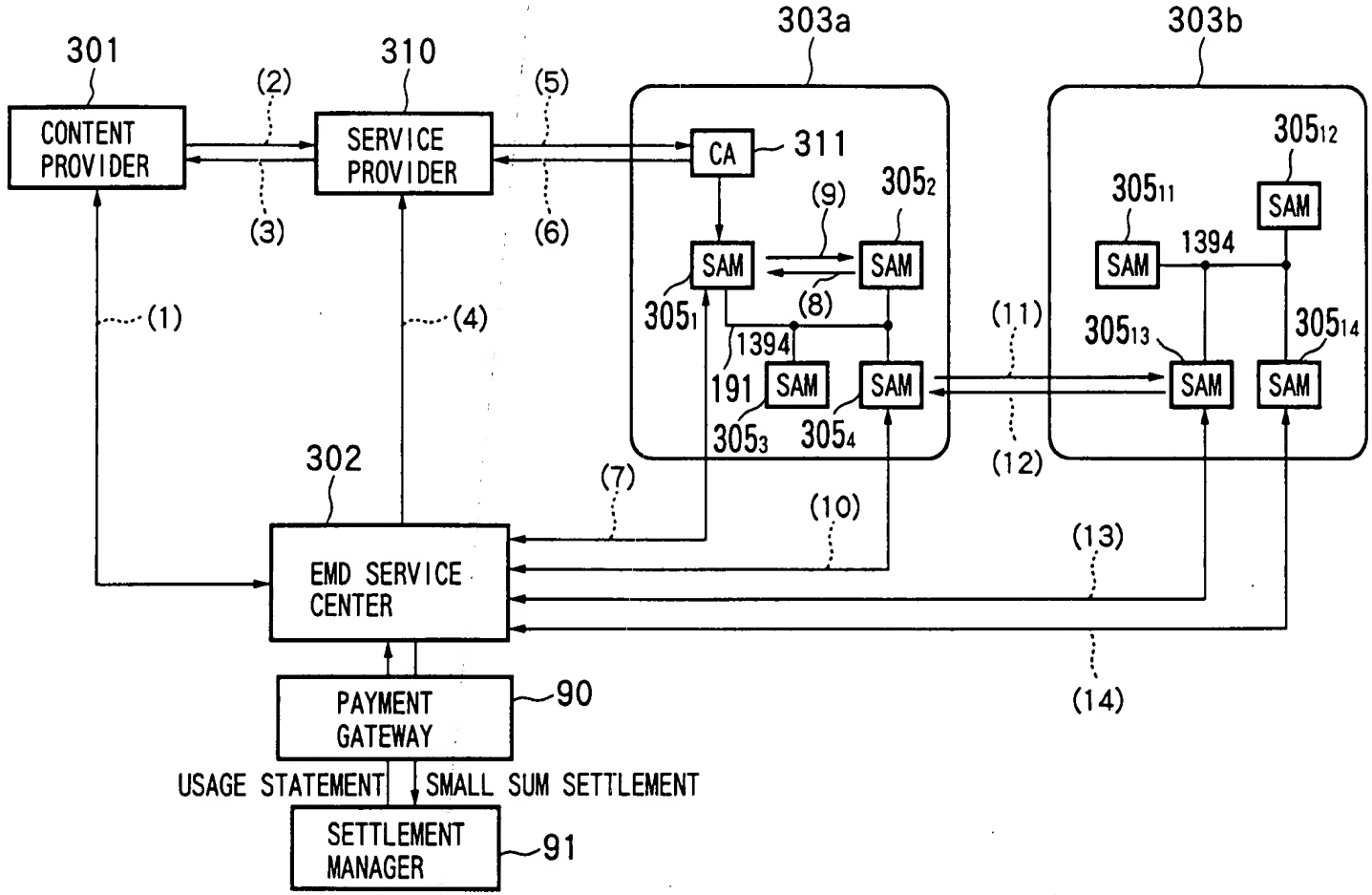

SAM
CA
USER HOME NETWORK
USAGE LOG DATA
SERVICE PROVIDER
USAGE LOG DATA
PAYMENT GATEWAY
SETTLEMENT MANAGER
EMD SERVICE CENTER (CLEARINGHOUSE)
CONTENT PROVIDER
PAYMENT GATEWAY
SETTLEMENT MANAGER
SETTLEMENT CLAIM DATA
ROUTE CERTIFICATE AUTHORITY

FIG.101



ACQUISITION ROUTE OF PUBLIC KEY CERTIFICATE

FIG.102

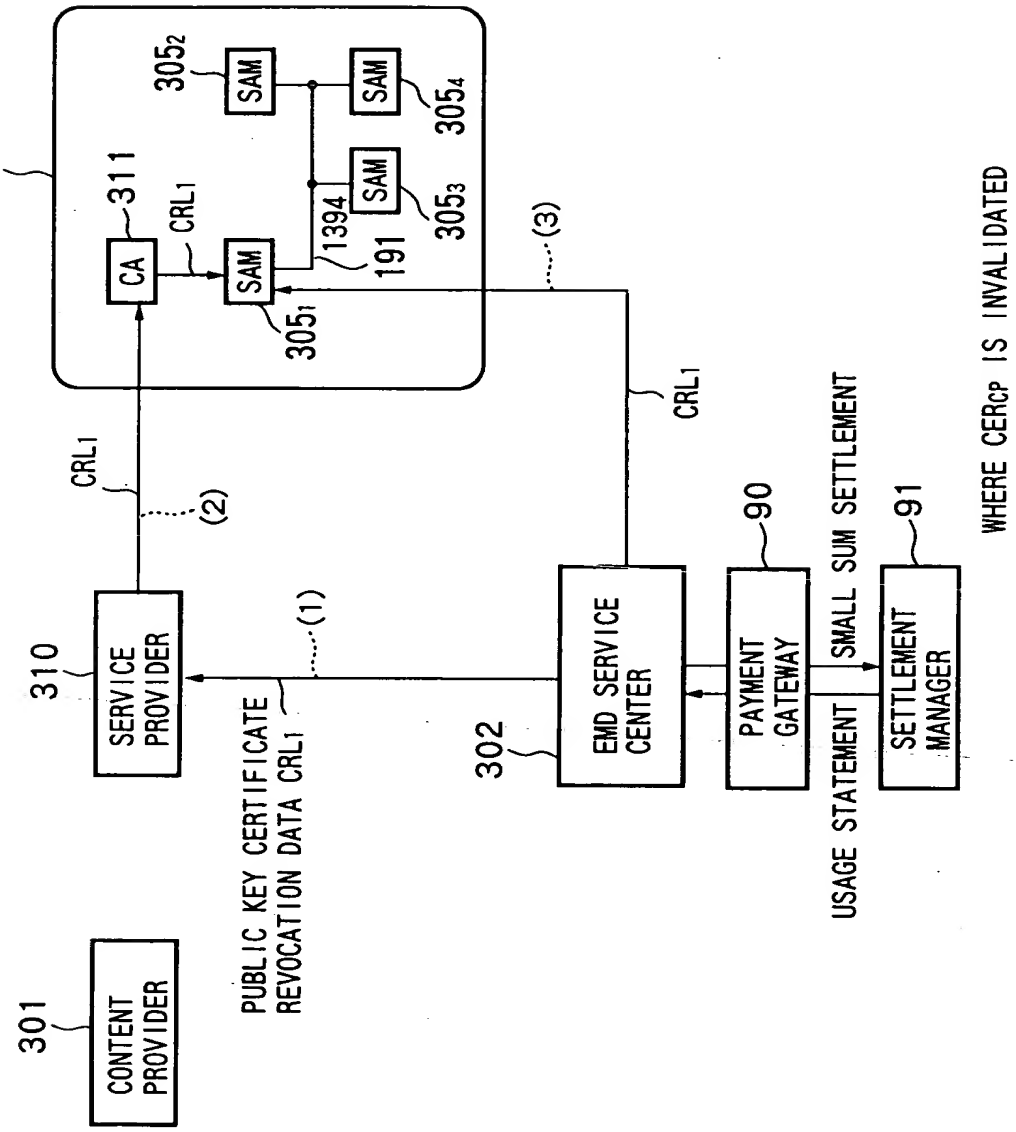

303
311
CA
CRL1
SAM
305₁
1394
191
SAM
305₂
SAM
305₃
SAM
305₄
(3)
CRL1
CRL1
(2)
310
SERVICE PROVIDER
(1)
PUBLIC KEY CERTIFICATE REVOCATION DATA CRL1
301
CONTENT PROVIDER
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
USAGE STATEMENT
91
SETTLEMENT MANAGER
WHERE CERCP IS INVALIDATED

FIG.103

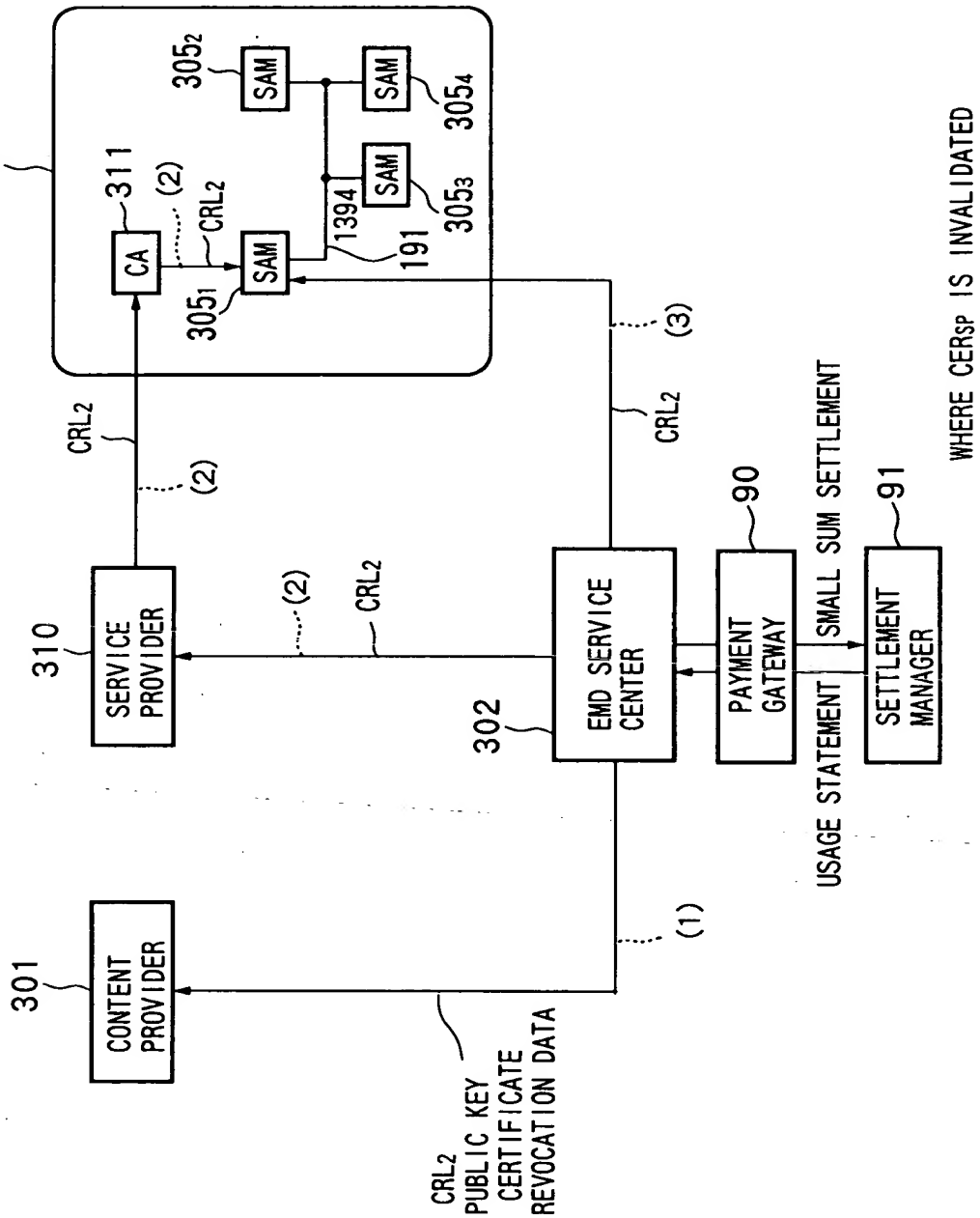

303
311
CA
(2)
CRL2
SAM
3051
3052
SAM
SAM
3053
SAM
3054
1394
191
(3)
CRL2
CRL2
(2)
310
SERVICE PROVIDER
(2)
CRL2
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT MANAGER
USAGE STATEMENT
WHERE CERSP IS INVALIDATED
301
CONTENT PROVIDER
(1)
CRL2
PUBLIC KEY CERTIFICATE REVOCATION DATA

FIG.104

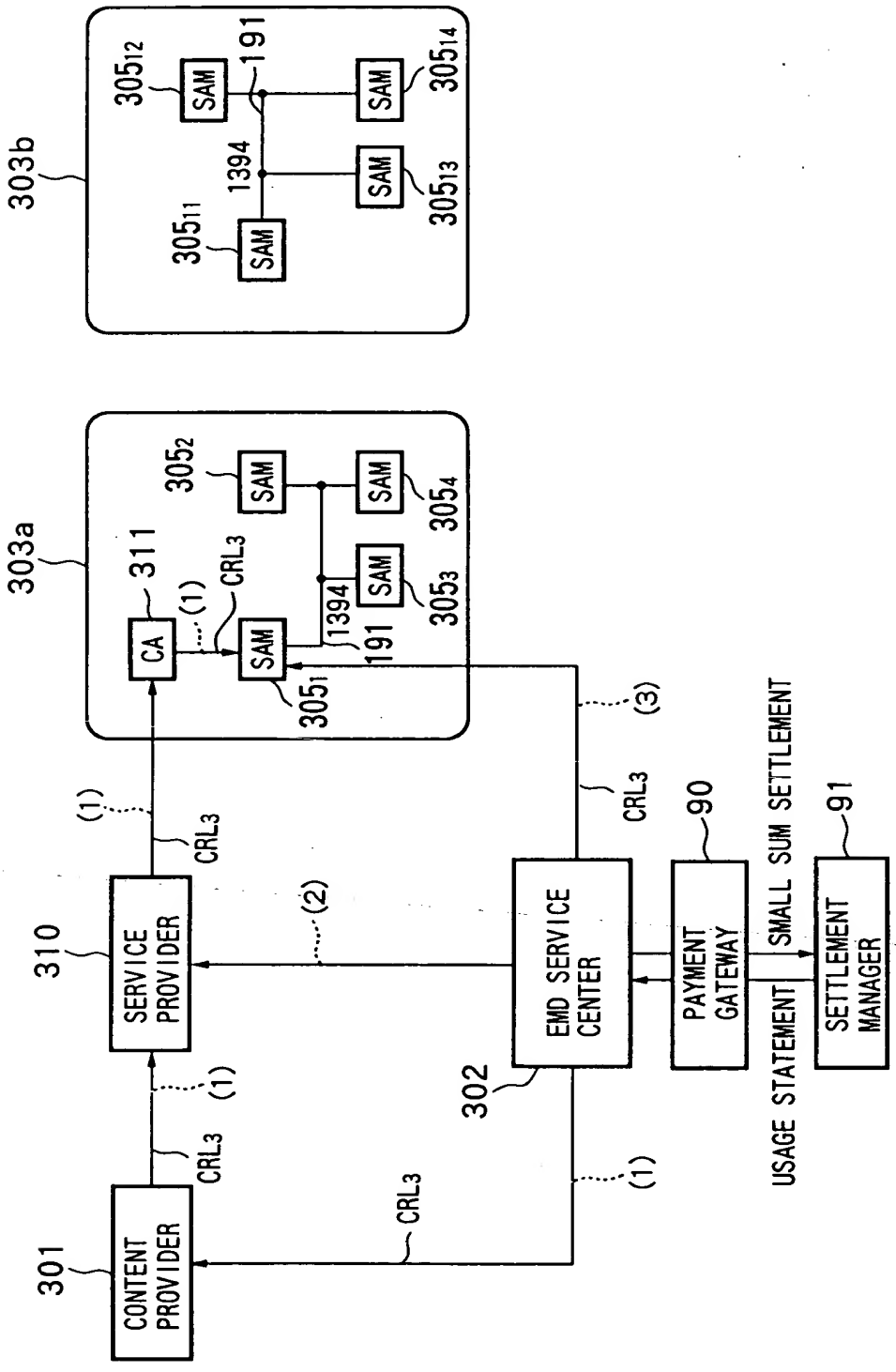

303b
305₁₂
SAM
191
SAM
305₁₄
1394
SAM
305₁₃
305₁₁
SAM
303a
305₂
SAM
SAM
305₄
311
CA
(1)
CRL3
SAM
1394
SAM
305₃
191
305₁
(3)
CRL3
(1)
CRL3
310
SERVICE PROVIDER
(2)
EMD SERVICE CENTER
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT MANAGER
(1)
CRL3
302
CRL3
(1)
301
CONTENT PROVIDER
USAGE STATEMENT
WHERE CERSAM2 IS INVALIDATED

FIG.105

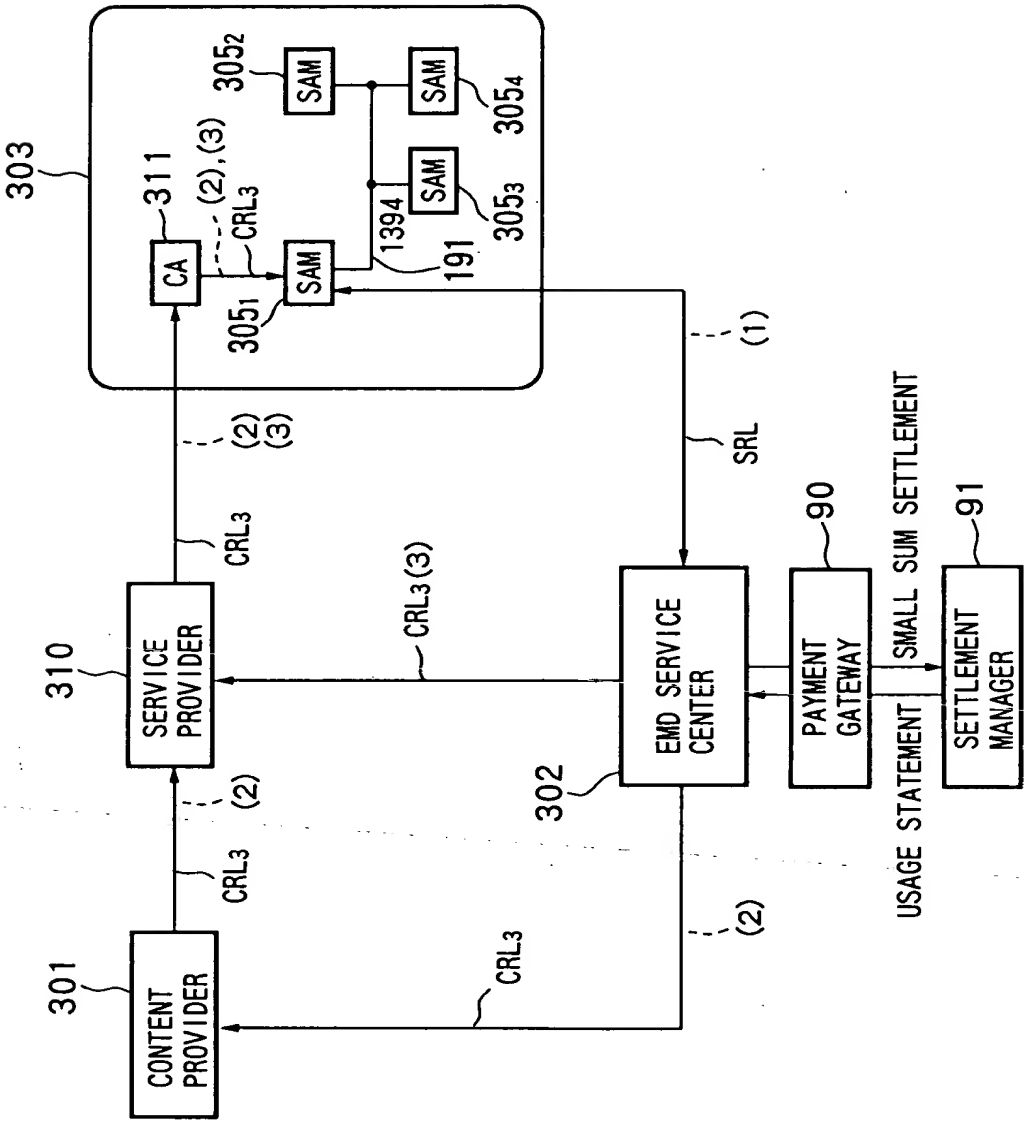

303
311
CA
(2),(3)
CRL3
SAM
3052
SAM
3054
SAM
3053
1394
191
SAM
3051
(1)
SRL
(2)
(3)
CRL3
310
SERVICE PROVIDER
CRL3(3)
EMD SERVICE CENTER
302
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT MANAGER
USAGE STATEMENT
(2)
CRL3
301
CONTENT PROVIDER
CRL3

FIG.106

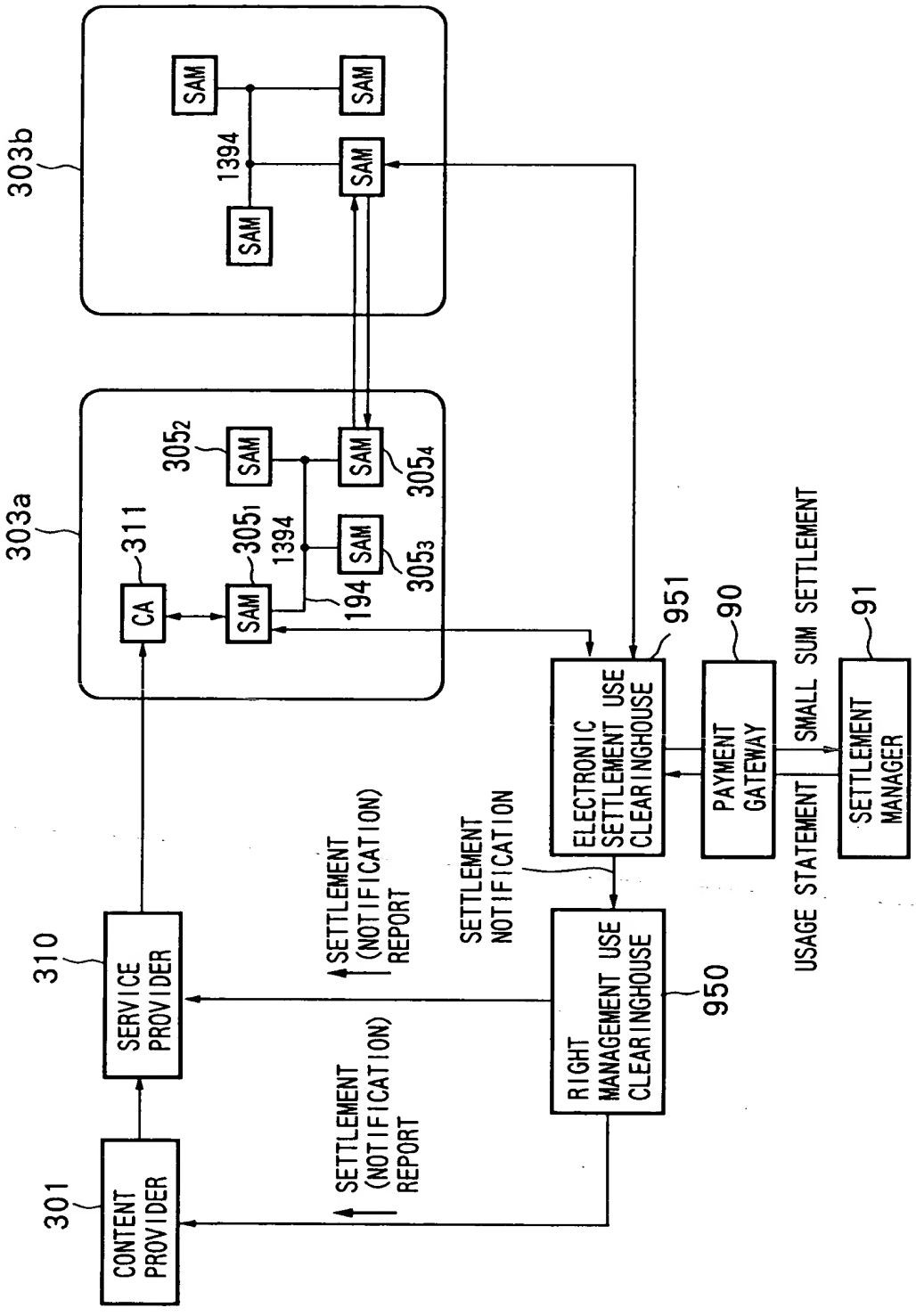

303b
SAM
SAM
1394
SAM
SAM
303a
305_2
SAM
SAM
305_4
311
CA
305_1
SAM
1394
SAM
305_3
194
951
ELECTRONIC SETTLEMENT USE CLEARINGHOUSE
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT MANAGER
USAGE STATEMENT
SETTLEMENT (NOTIFICATION) REPORT
SETTLEMENT NOTIFICATION
310
SERVICE PROVIDER
RIGHT MANAGEMENT USE CLEARINGHOUSE
950
SETTLEMENT (NOTIFICATION) REPORT
301
CONTENT PROVIDER

FIG.107

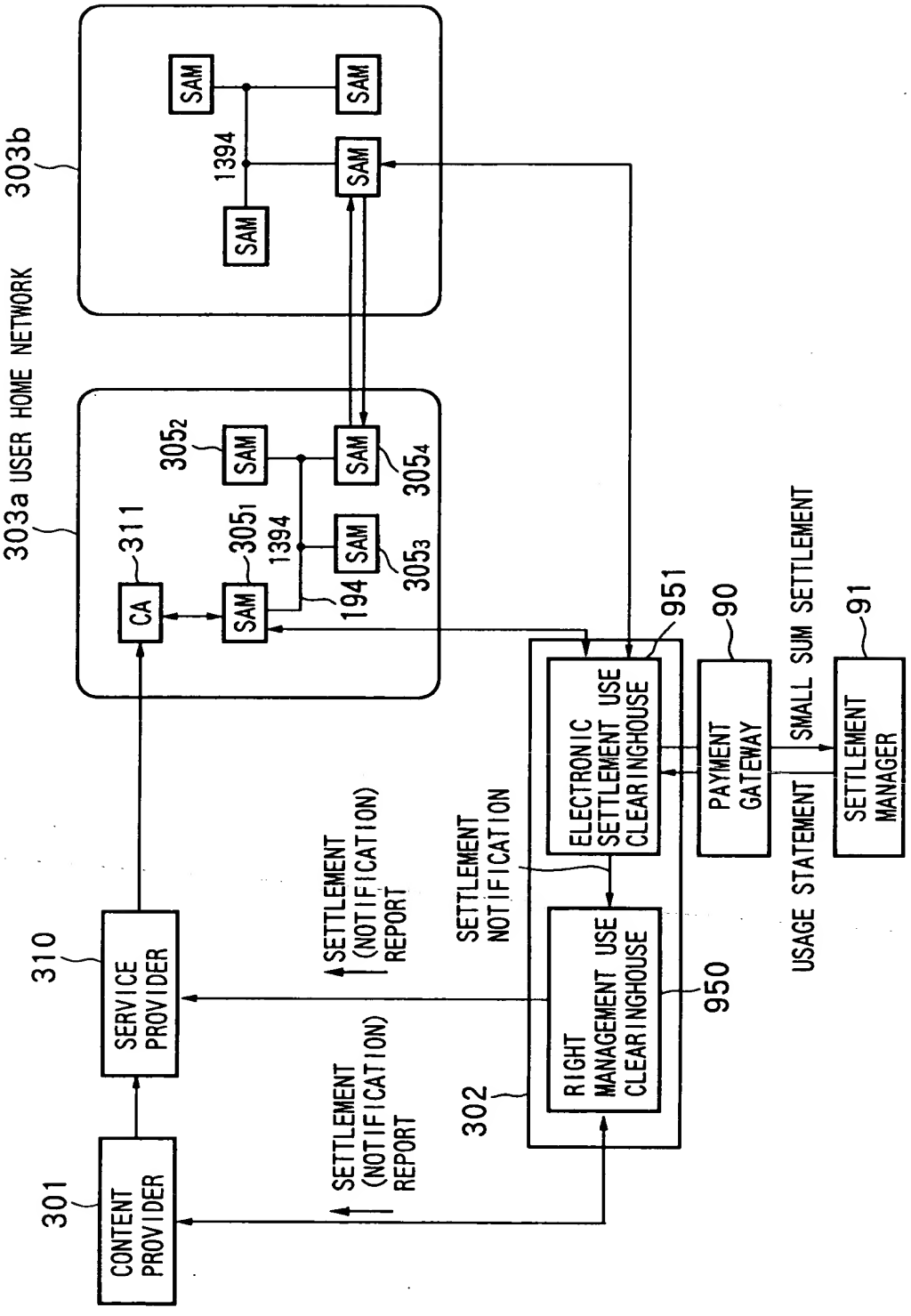

303b
SAM
SAM
1394
SAM
SAM
303a USER HOME NETWORK
305_2
SAM
SAM
305_4
311
CA
305_1
SAM
1394
SAM
305_3
194
951
90
91
ELECTRONIC SETTLEMENT USE CLEARINGHOUSE
PAYMENT GATEWAY
SETTLEMENT MANAGER
SMALL SUM SETTLEMENT
USAGE STATEMENT
SETTLEMENT NOTIFICATION
SETTLEMENT (NOTIFICATION) REPORT
310
SERVICE PROVIDER
950
RIGHT MANAGEMENT USE CLEARINGHOUSE
302
SETTLEMENT (NOTIFICATION) REPORT
301
CONTENT PROVIDER

FIG.108

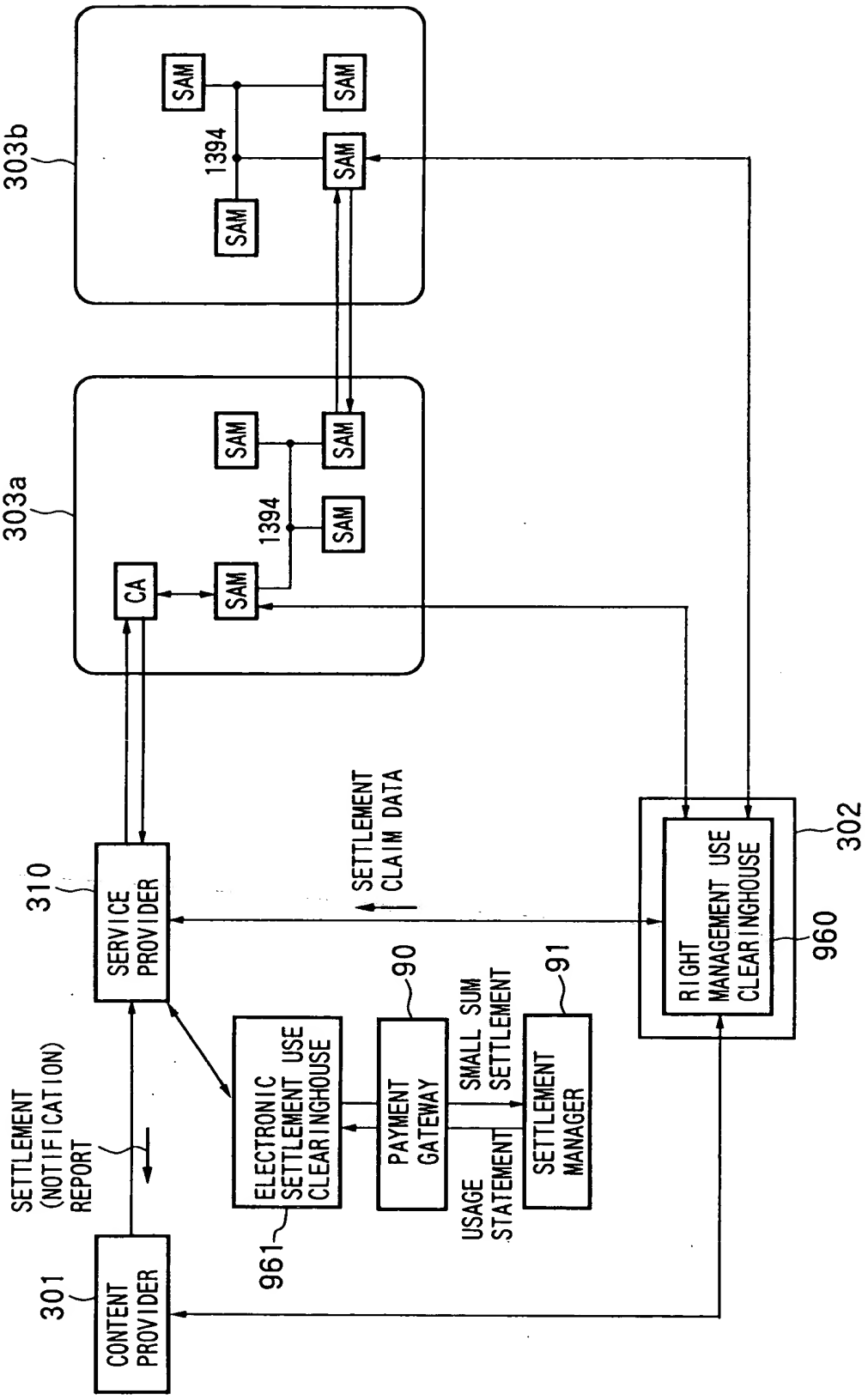

303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
SETTLEMENT CLAIM DATA
310
SERVICE PROVIDER
302
RIGHT MANAGEMENT USE CLEARINGHOUSE
960
90
91
SETTLEMENT (NOTIFICATION) REPORT
ELECTRONIC SETTLEMENT USE CLEARINGHOUSE
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
SETTLEMENT MANAGER
USAGE STATEMENT
961
301
CONTENT PROVIDER

FIG.109

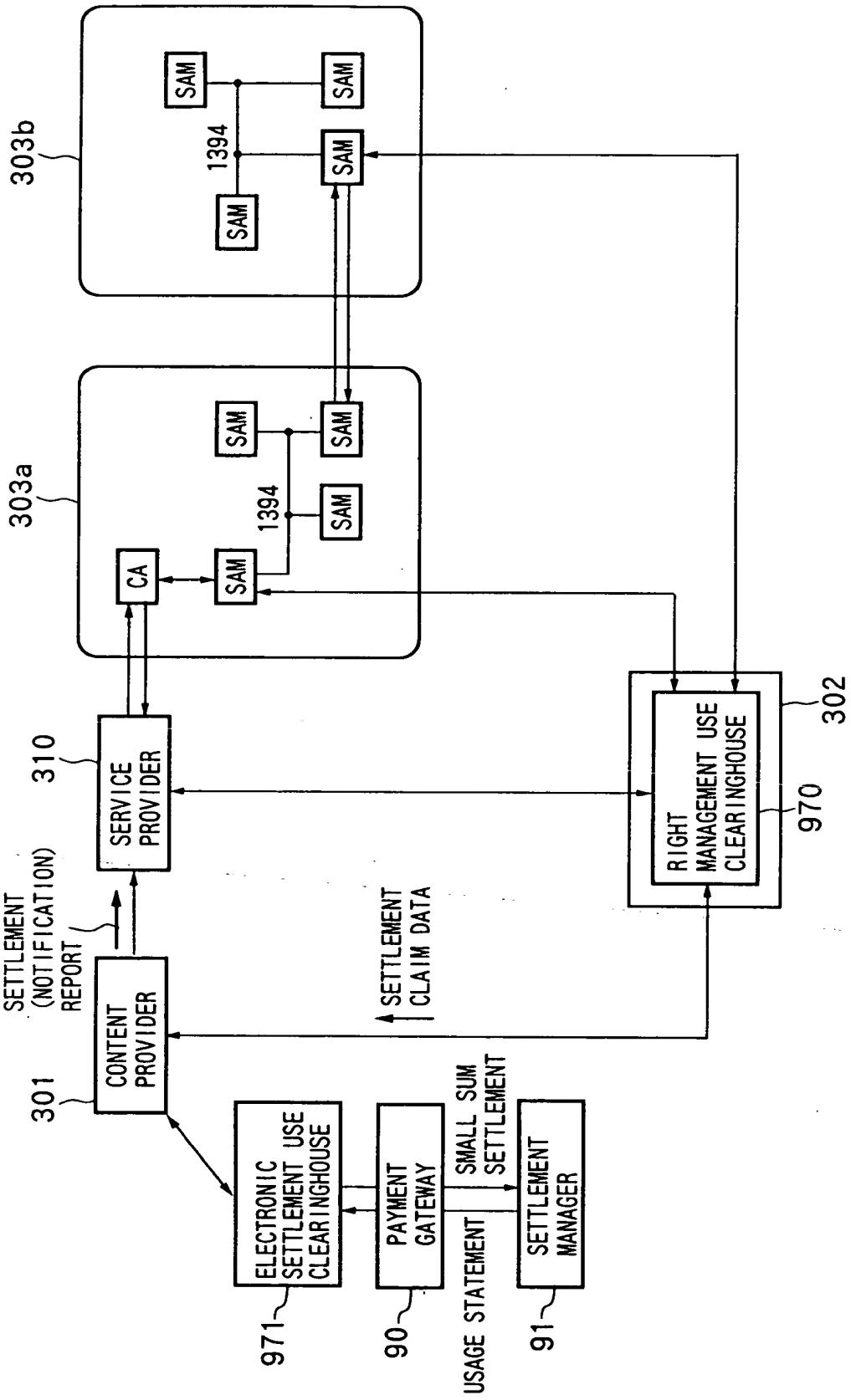

303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
310
SERVICE PROVIDER
302
RIGHT MANAGEMENT USE CLEARINGHOUSE
970
SETTLEMENT (NOTIFICATION) REPORT
SETTLEMENT CLAIM DATA
301
CONTENT PROVIDER
ELECTRONIC SETTLEMENT USE CLEARINGHOUSE
971
PAYMENT GATEWAY
90
SMALL SUM SETTLEMENT
USAGE STATEMENT
SETTLEMENT MANAGER
91

FIG.110

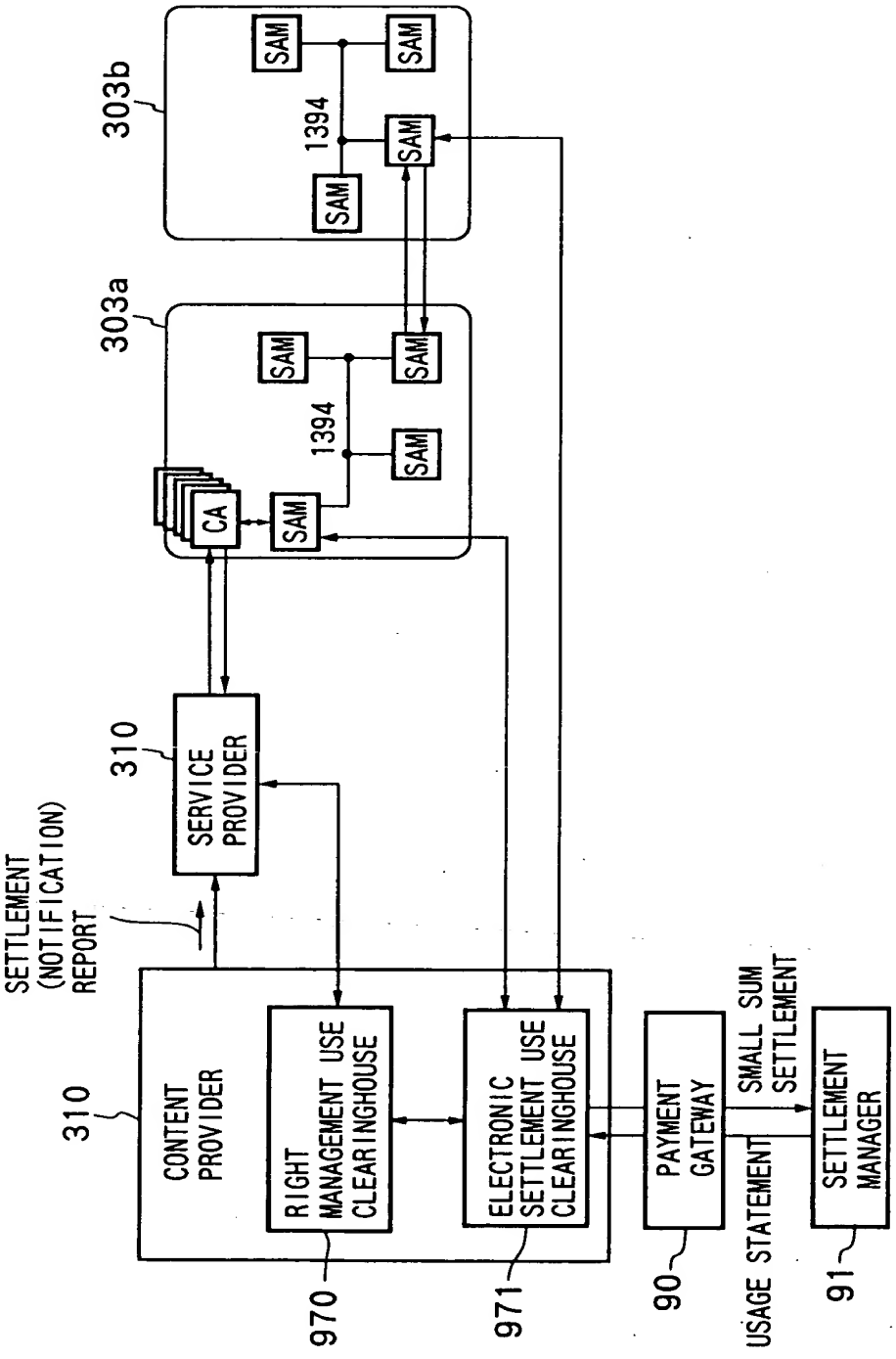

303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
310
SERVICE PROVIDER
SETTLEMENT (NOTIFICATION) REPORT
310
CONTENT PROVIDER
RIGHT MANAGEMENT USE CLEARINGHOUSE
ELECTRONIC SETTLEMENT USE CLEARINGHOUSE
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
SETTLEMENT MANAGER
970
971
90
USAGE STATEMENT
91

FIG.111

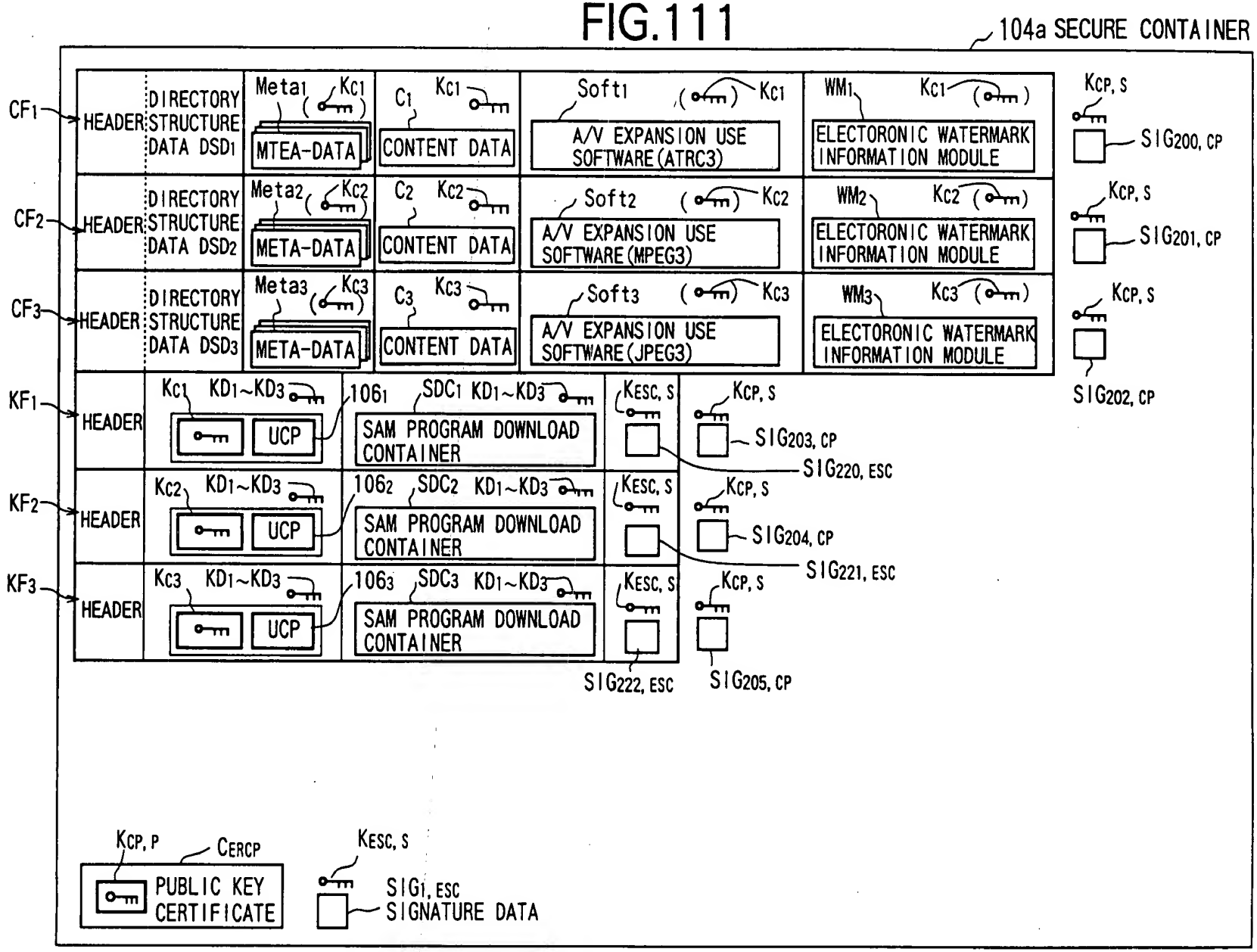


FIG.112

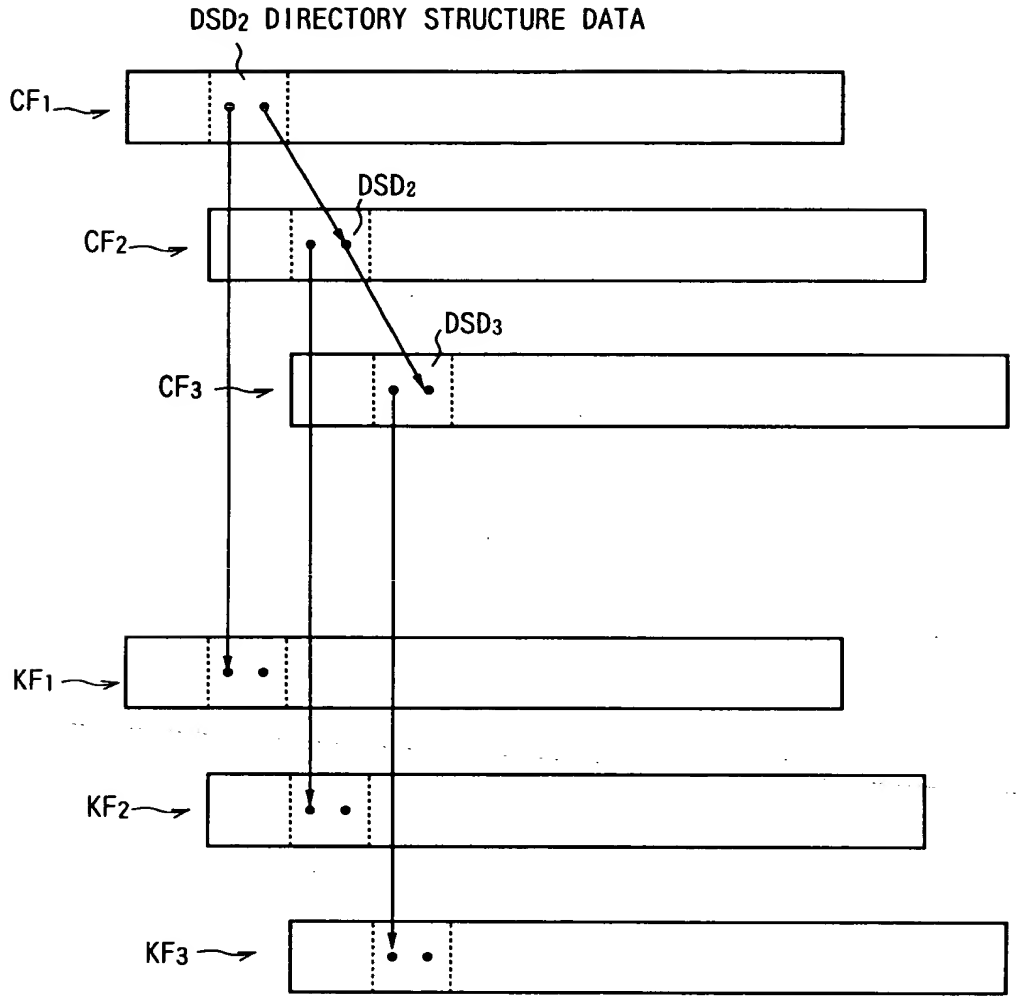

DSD2 DIRECTORY STRUCTURE DATA
CF1
DSD2
CF2
DSD3
CF3
KF1
KF2
KF3

FIG.113

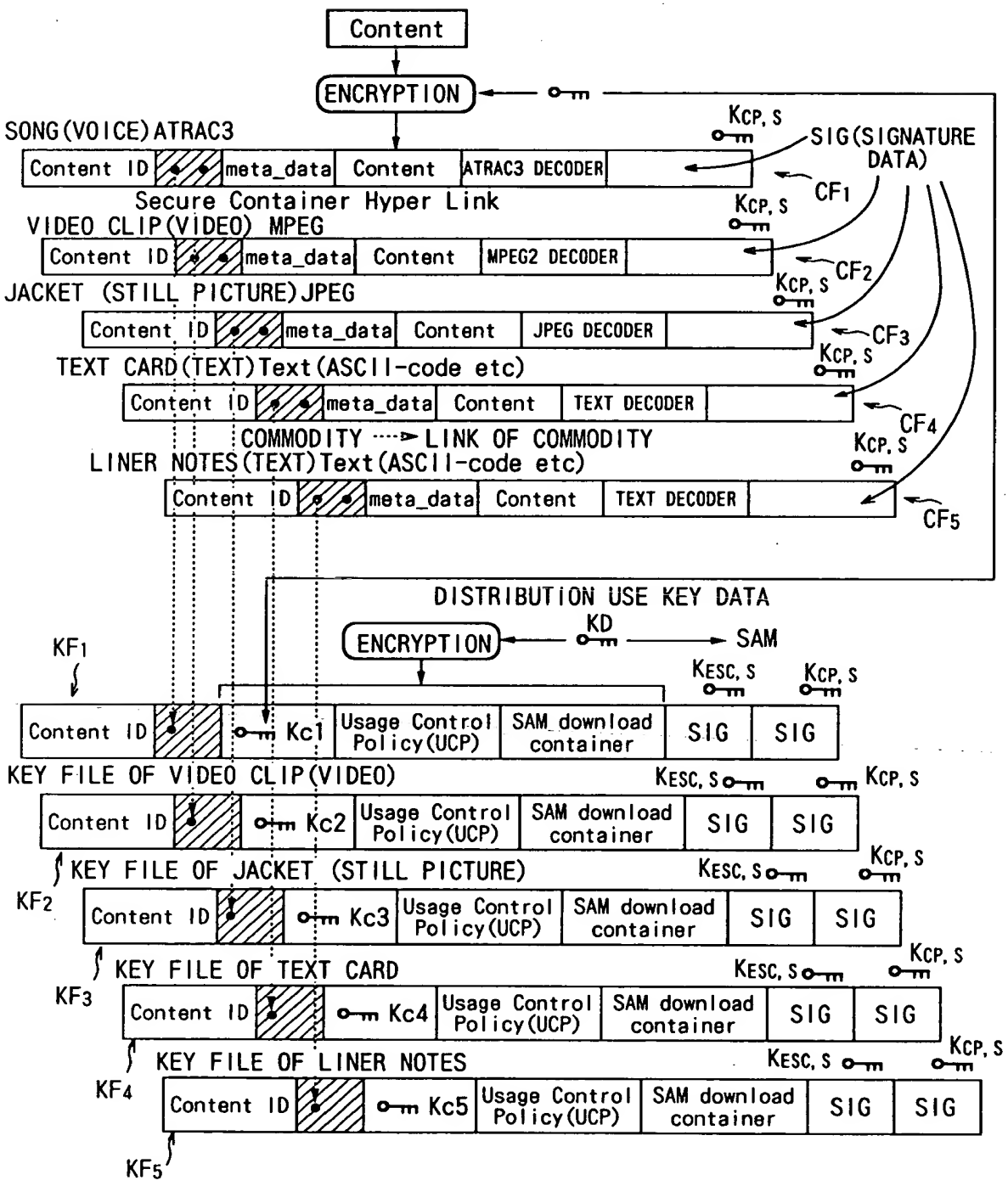

Content
ENCRYPTION
SONG(VOICE)ATRAC3
KCP, S
SIG(SIGNATURE DATA)
Content ID
meta_data
Content
ATRAC3 DECODER
CF1
Secure Container Hyper Link
VIDEO CLIP(VIDEO) MPEG
MPEG2 DECODER
CF2
JACKET (STILL PICTURE)JPEG
JPEG DECODER
CF3
TEXT CARD(TEXT)Text(ASCII-code etc)
TEXT DECODER
CF4
COMMODITY ····► LINK OF COMMODITY
LINER NOTES(TEXT)Text(ASCII-code etc)
CF5
DISTRIBUTION USE KEY DATA
KD
SAM
KF1
KESC, S
Kc1
Usage Control Policy(UCP)
SAM download container
SIG
KEY FILE OF VIDEO CLIP(VIDEO)
Kc2
KEY FILE OF JACKET (STILL PICTURE)
KF2
Kc3
KEY FILE OF TEXT CARD
KF3
Kc4
KEY FILE OF LINER NOTES
KF4
Kc5
KF5

FIG.114

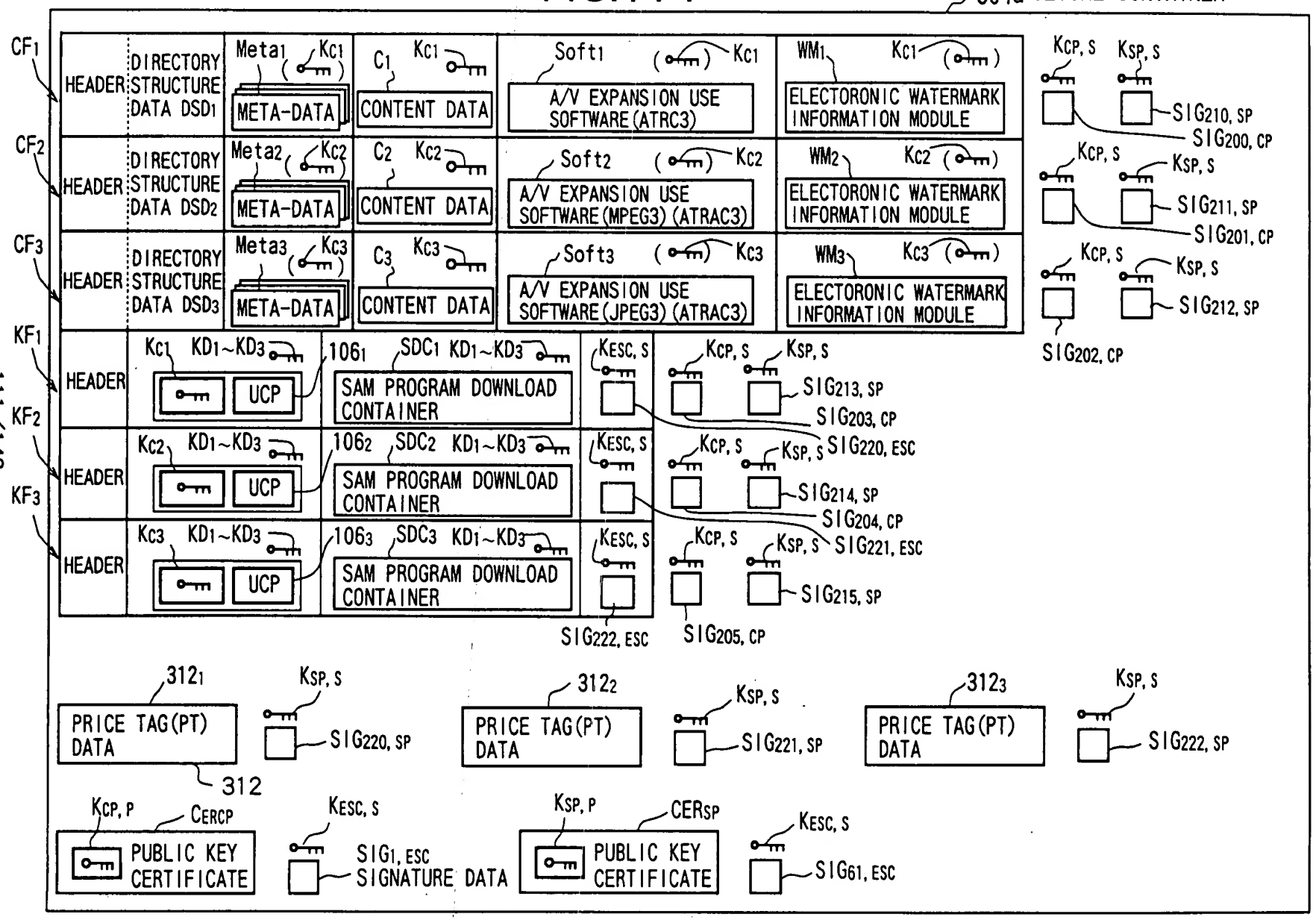


FIG.115

DATA FORMAT OF SECURE CONTAINER(COMPOSITE TYPE)-①

BASIC STRUCTURE

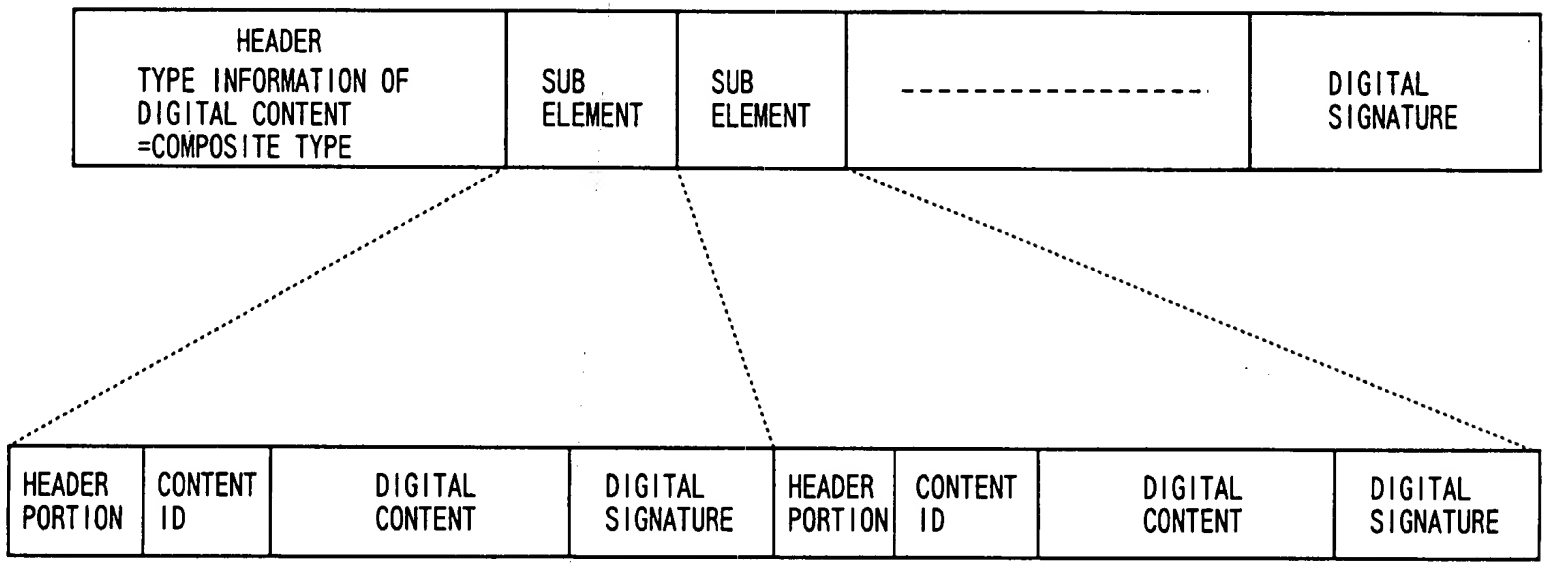


FIG.116

DATA FORMAT OF SECURE CONTAINER(COMPOSITE TYPE)-②

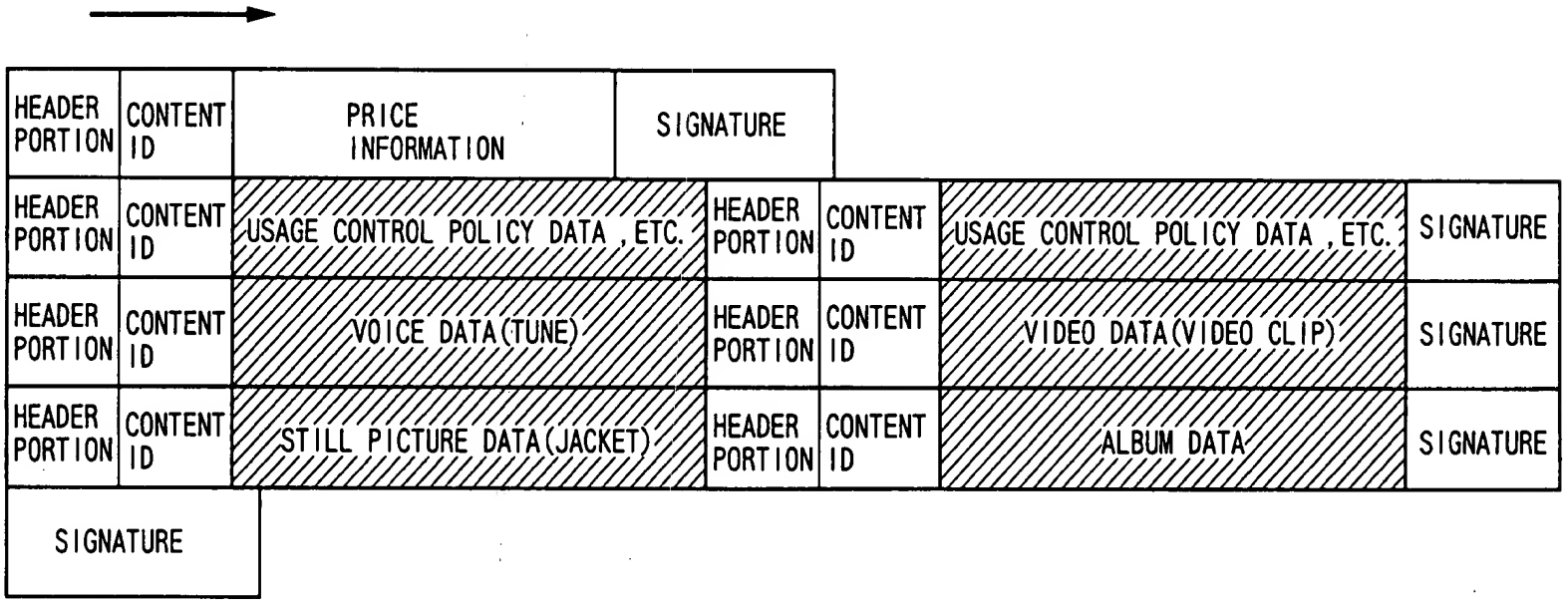


FIG.117

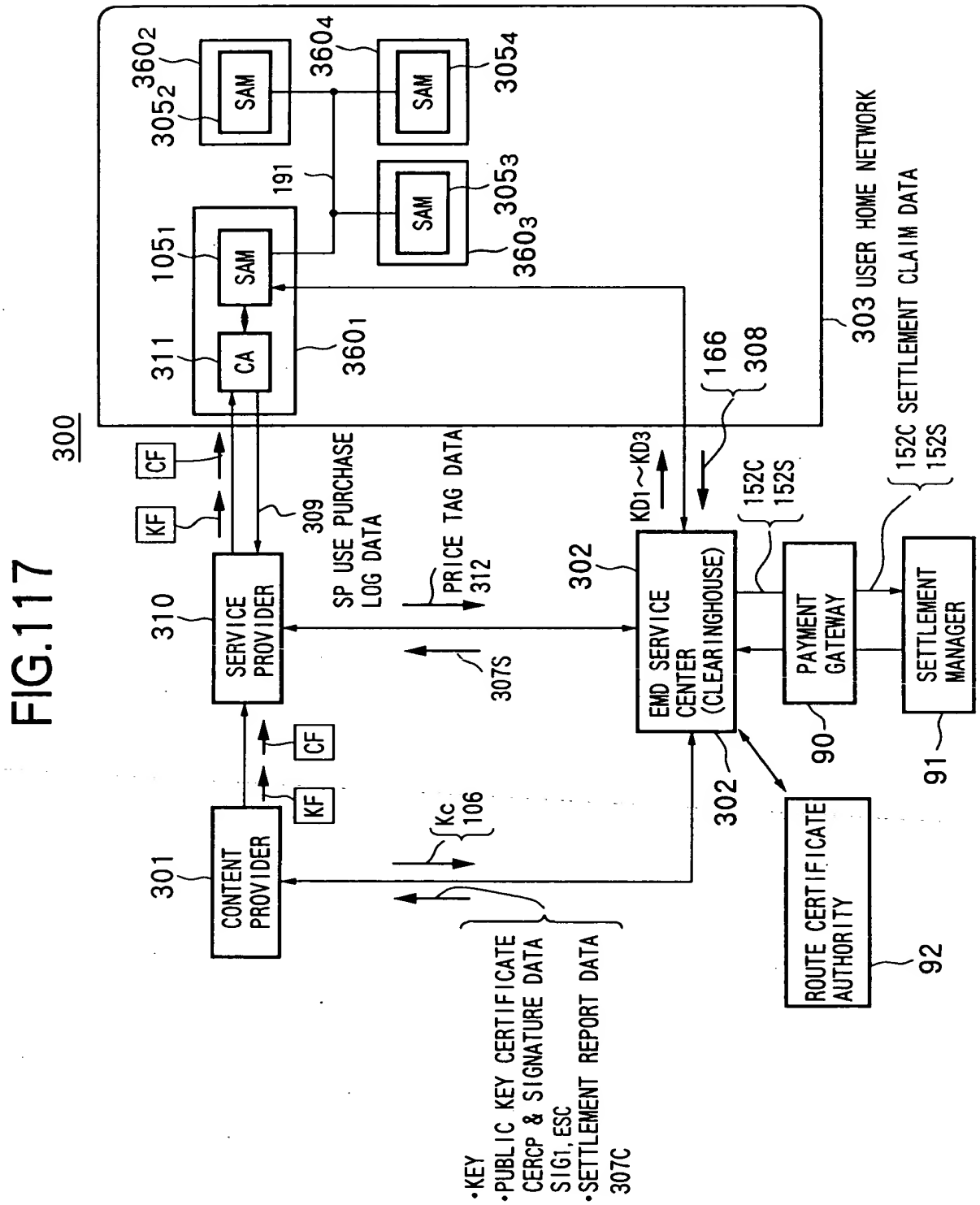

300
303 USER HOME NETWORK
SAM
CA
311
191
166
308
309
SP USE PURCHASE LOG DATA
PRICE TAG DATA
312
307S
SERVICE PROVIDER
310
CONTENT PROVIDER
301
CF
KF
Kc
106
KD1~KD3
302
EMD SERVICE CENTER (CLEARINGHOUSE)
152C
152S
152C SETTLEMENT CLAIM DATA
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
ROUTE CERTIFICATE AUTHORITY
92
•KEY
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 307C

FIG.118

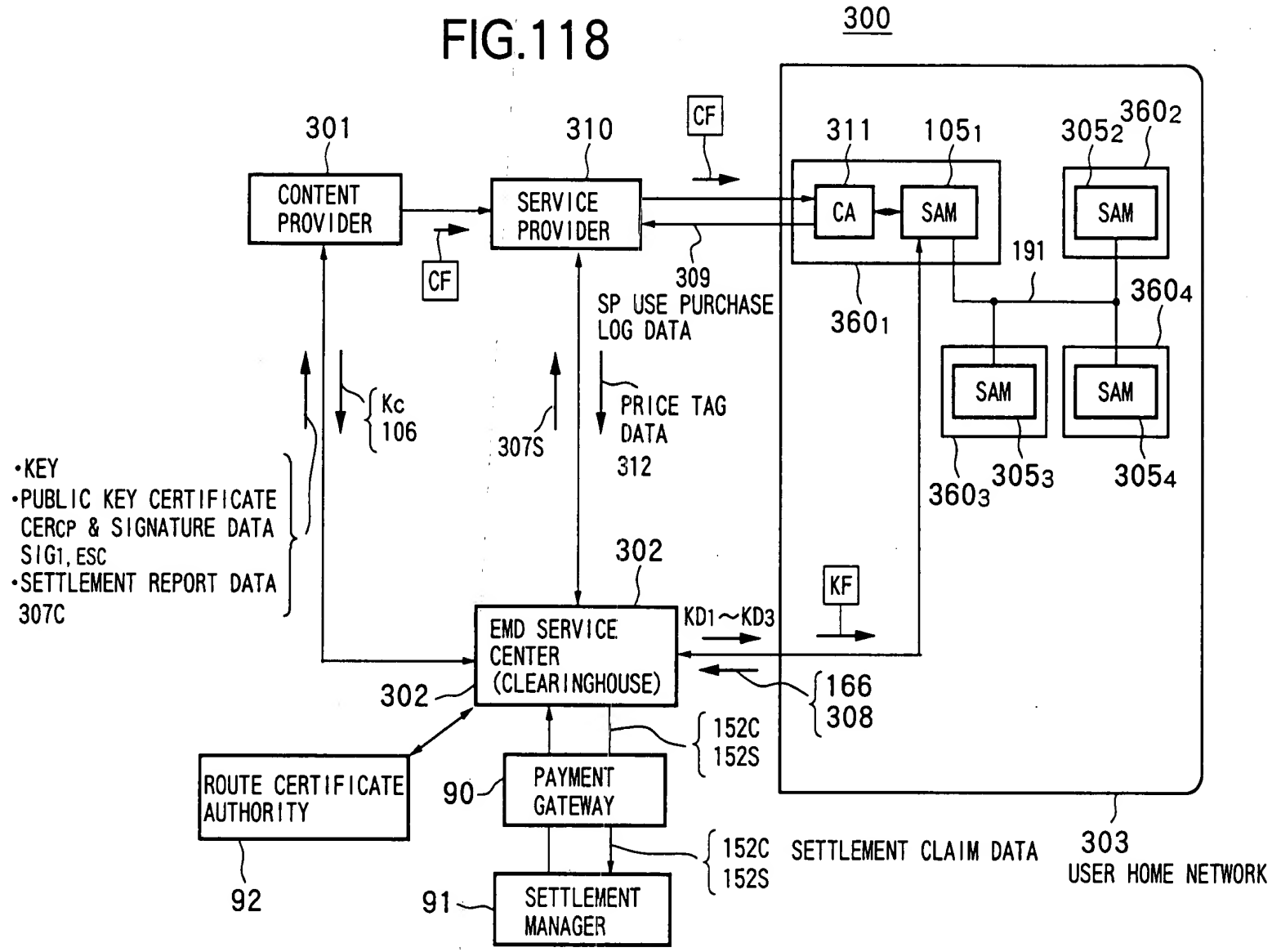


FIG.119

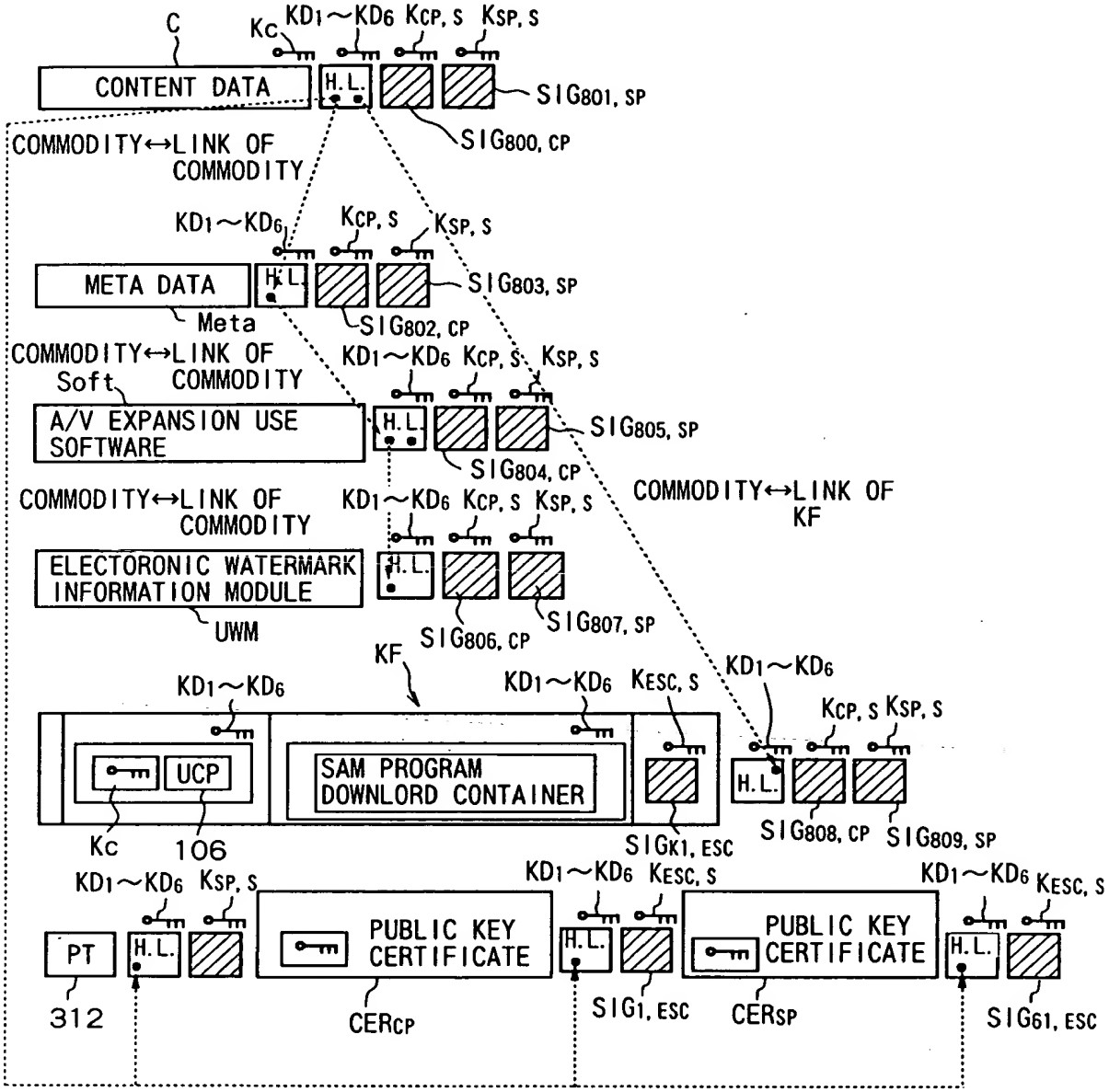

C
Kc
KD1～KD6 KCP, S KSP, S
CONTENT DATA
H.L.
SIG801, SP
SIG800, CP
COMMODITY↔LINK OF COMMODITY
KD1～KD6
KCP, S
KSP, S
META DATA
H.L.
SIG803, SP
Meta
SIG802, CP
COMMODITY↔LINK OF COMMODITY
Soft
KD1～KD6 KCP, S KSP, S
A/V EXPANSION USE SOFTWARE
H.L.
SIG805, SP
SIG804, CP
COMMODITY↔LINK OF COMMODITY
KD1～KD6 KCP, S KSP, S
COMMODITY↔LINK OF KF
ELECTORONIC WATERMARK INFORMATION MODULE
H.L.
UWM
SIG806, CP
SIG807, SP
KF
KD1～KD6
KD1～KD6 KESC, S
KD1～KD6
KCP, S KSP, S
UCP
SAM PROGRAM DOWNLORD CONTAINER
H.L.
Kc
106
SIGK1, ESC
SIG808, CP
SIG809, SP
KD1～KD6 KSP, S
KD1～KD6 KESC, S
KD1～KD6 KESC, S
PT
H.L.
PUBLIC KEY CERTIFICATE
H.L.
PUBLIC KEY CERTIFICATE
H.L.
312
CERCP
SIG1, ESC
CERSP
SIG61, ESC

FIG.120

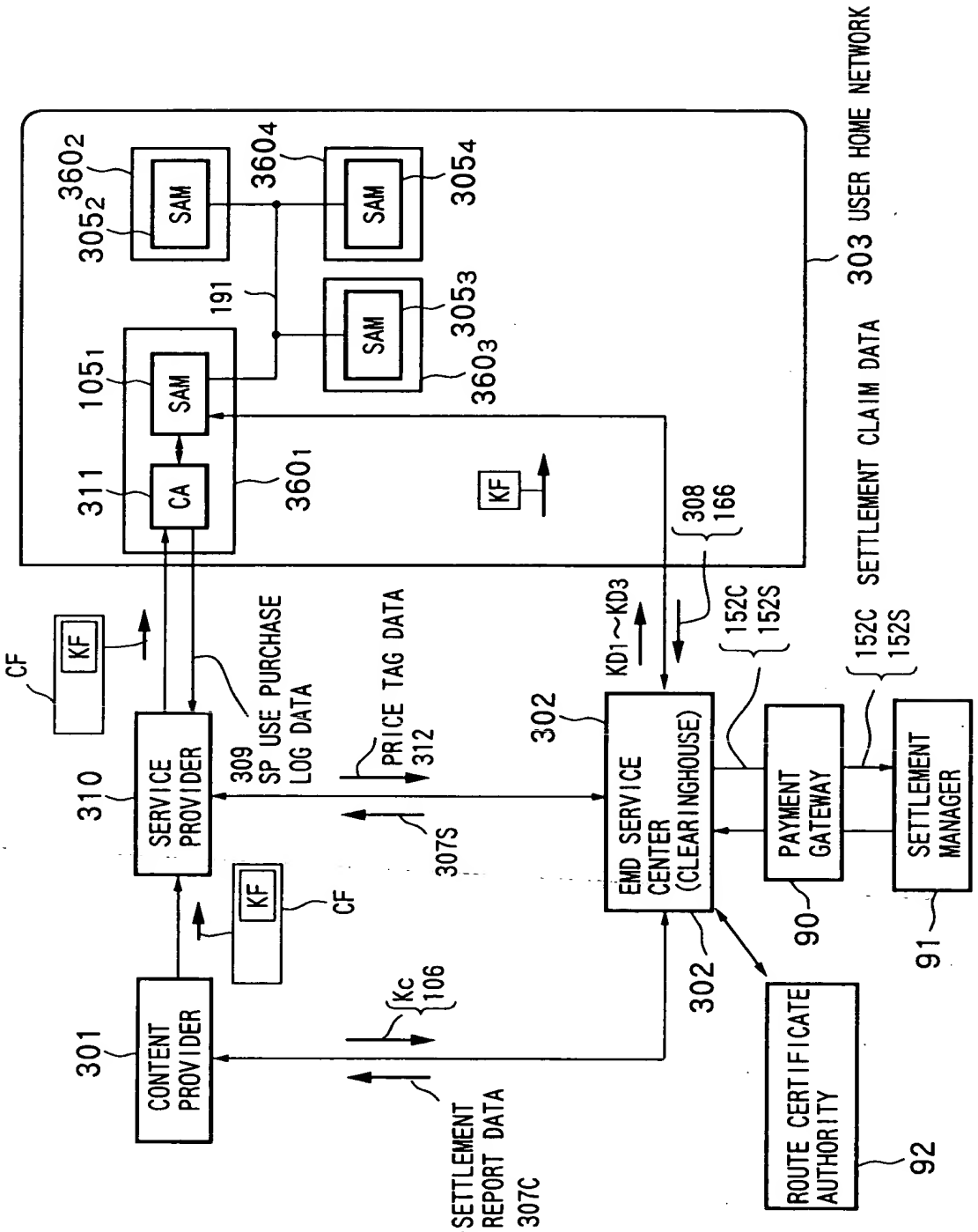

303 USER HOME NETWORK
SETTLEMENT CLAIM DATA
SAM
CA
KF
CF
SERVICE PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
ROUTE CERTIFICATE AUTHORITY
SP USE PURCHASE LOG DATA
PRICE TAG DATA
SETTLEMENT REPORT DATA
KD1~KD3
Kc
191
301
302
303
305
310
311
90
91
92
106
152C
152S
166
307C
307S
308
309
312

FIG.121

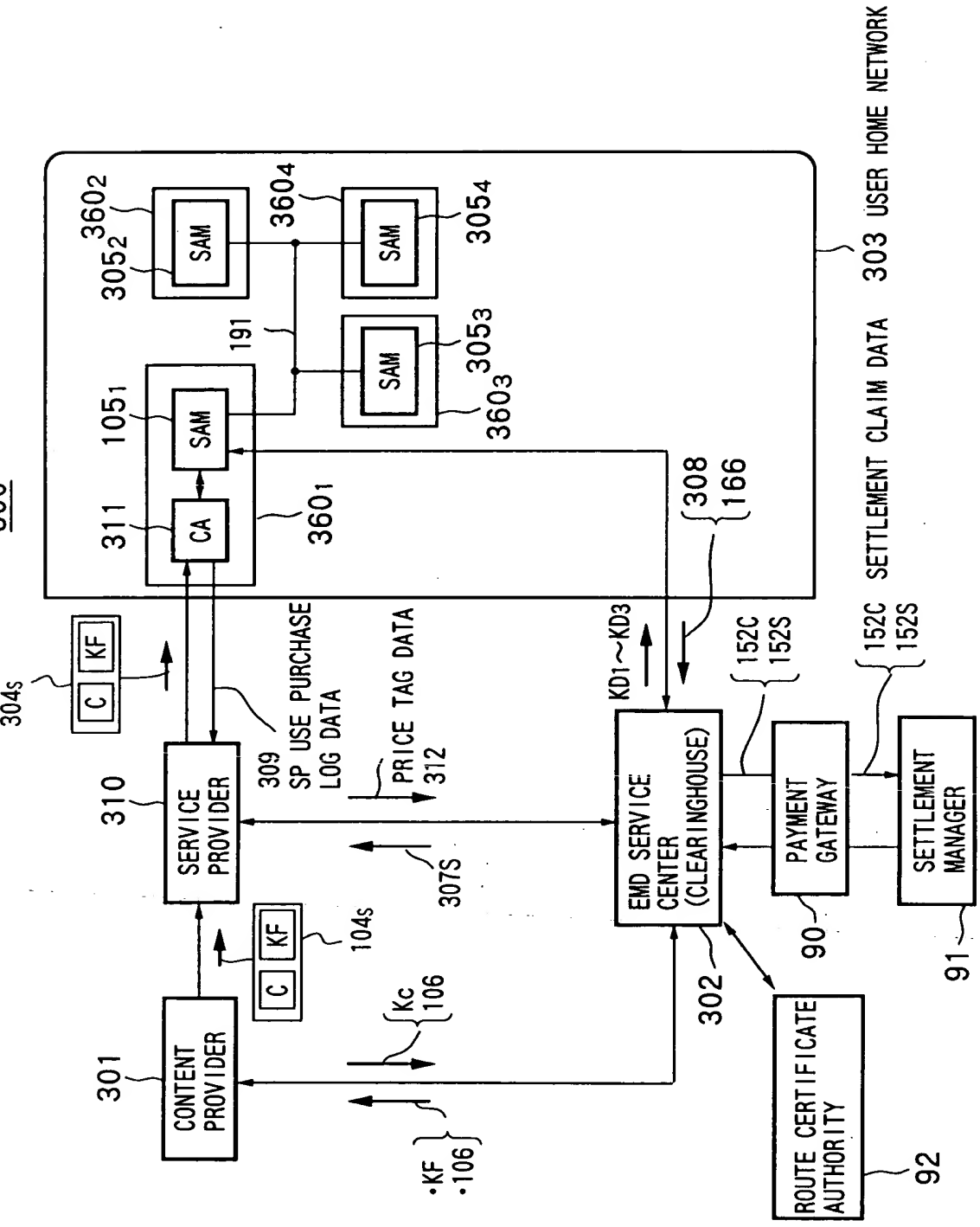

300
303 USER HOME NETWORK
SETTLEMENT CLAIM DATA
SAM
CA
C
KF
191
311
105₁
360₁
360₂
360₃
360₄
305₂
305₃
305₄
304s
308
166
309
SP USE PURCHASE LOG DATA
PRICE TAG DATA
312
307S
310
SERVICE PROVIDER
104s
Kc
106
301
CONTENT PROVIDER
•KF
•106
KD1~KD3
152C
152S
EMD SERVICE CENTER (CLEARINGHOUSE)
302
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
ROUTE CERTIFICATE AUTHORITY
92

FIG.122

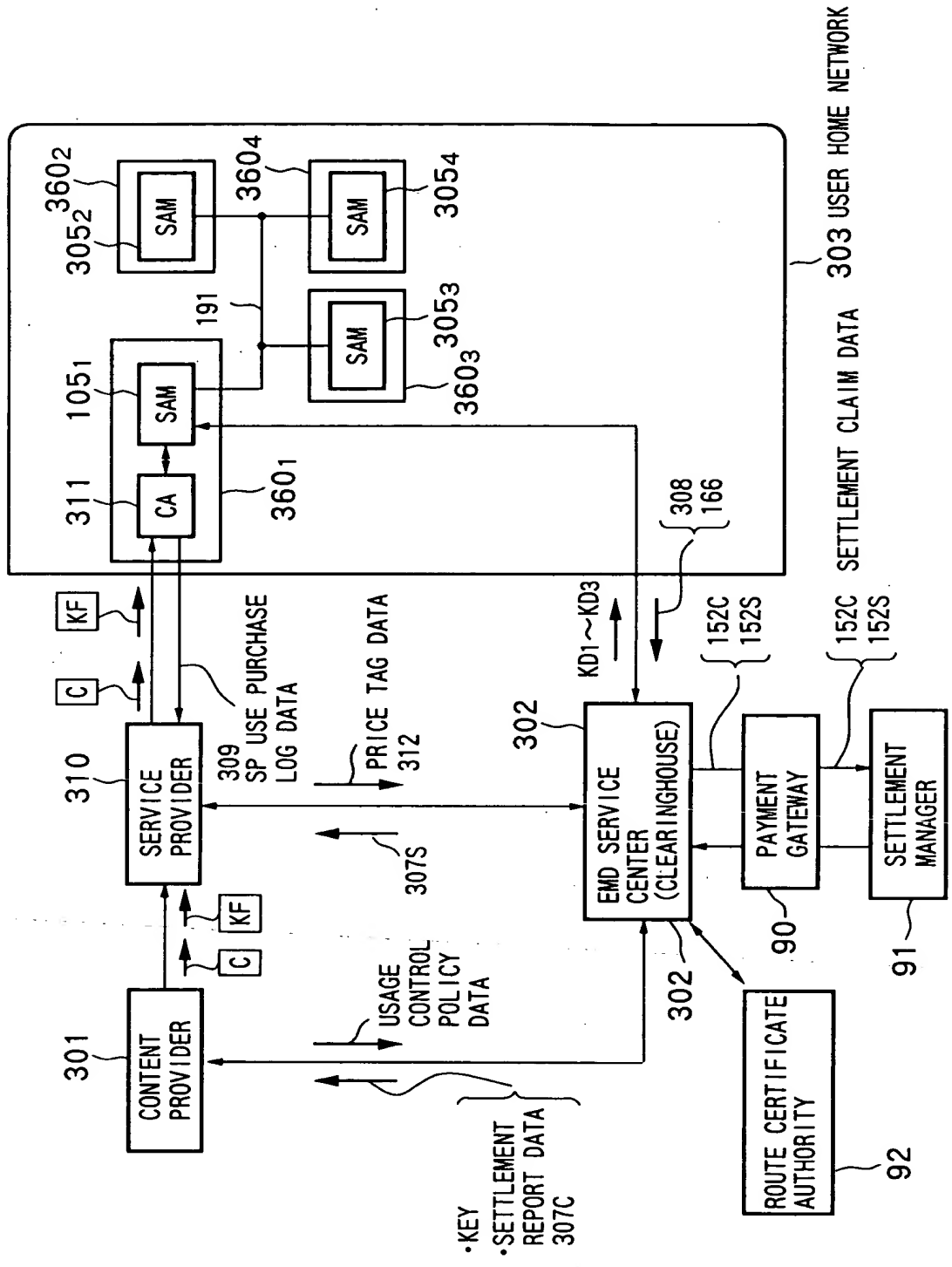

300
303 USER HOME NETWORK
SETTLEMENT CLAIM DATA
SAM
CA
KF
C
191
311
310
SERVICE PROVIDER
309 SP USE PURCHASE LOG DATA
PRICE TAG DATA 312
307S
KD1~KD3
308
166
152C
152S
302
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
90
91
301
CONTENT PROVIDER
USAGE CONTROL POLICY DATA
•KEY
•SETTLEMENT REPORT DATA 307C
ROUTE CERTIFICATE AUTHORITY
92

FIG.123

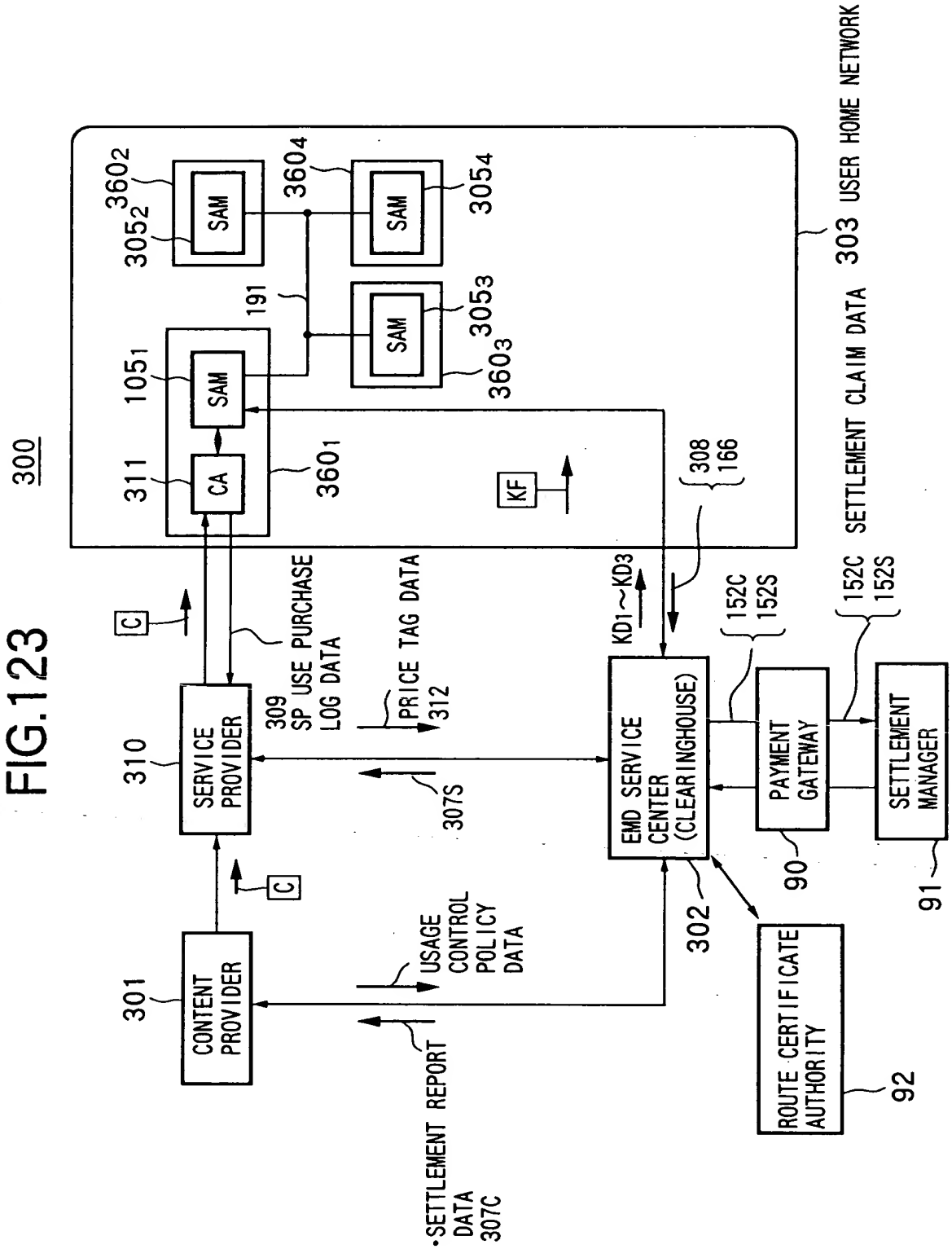

300
303 USER HOME NETWORK
SETTLEMENT CLAIM DATA
SAM
CA
KF
C
SERVICE PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
PAYMENT GATEWAY
SETTLEMENT MANAGER
ROUTE CERTIFICATE AUTHORITY
SP USE PURCHASE LOG DATA
PRICE TAG DATA
USAGE CONTROL POLICY DATA
SETTLEMENT REPORT DATA
KD1~KD3
152C
152S
308
166
191
310
309
312
307S
307C
301
302
90
91
92

FIG.124

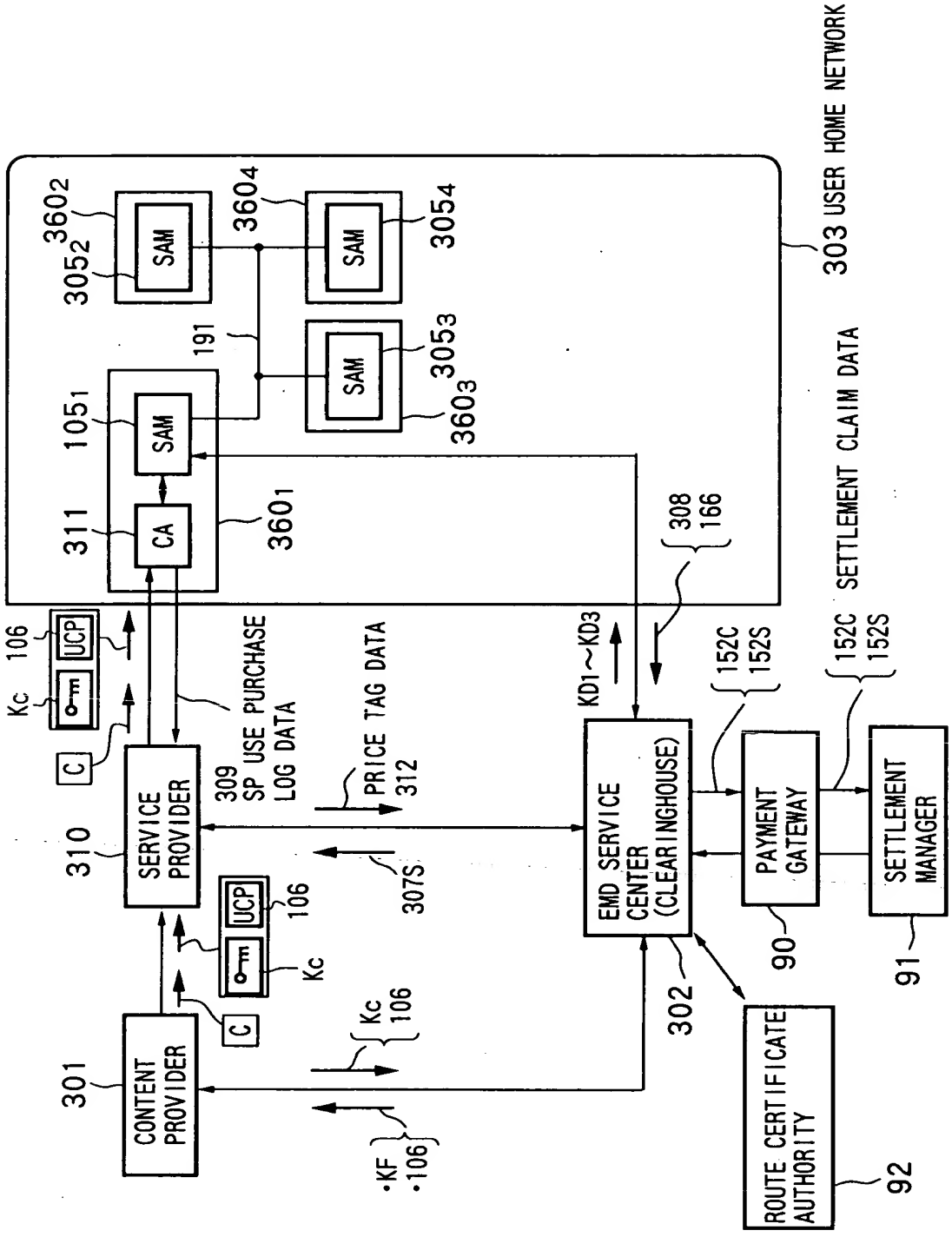

300
303 USER HOME NETWORK
SAM
CA
UCP
C
Kc
106
311
105₁
360₁
360₂
360₃
360₄
305₂
305₃
305₄
191
308
166
SETTLEMENT CLAIM DATA
152C
152S
KD1~KD3
SP USE PURCHASE LOG DATA
309
PRICE TAG DATA
312
307S
310
SERVICE PROVIDER
EMD SERVICE CENTER (CLEARINGHOUSE)
302
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
301
CONTENT PROVIDER
•KF
•106
ROUTE CERTIFICATE AUTHORITY
92

FIG.125

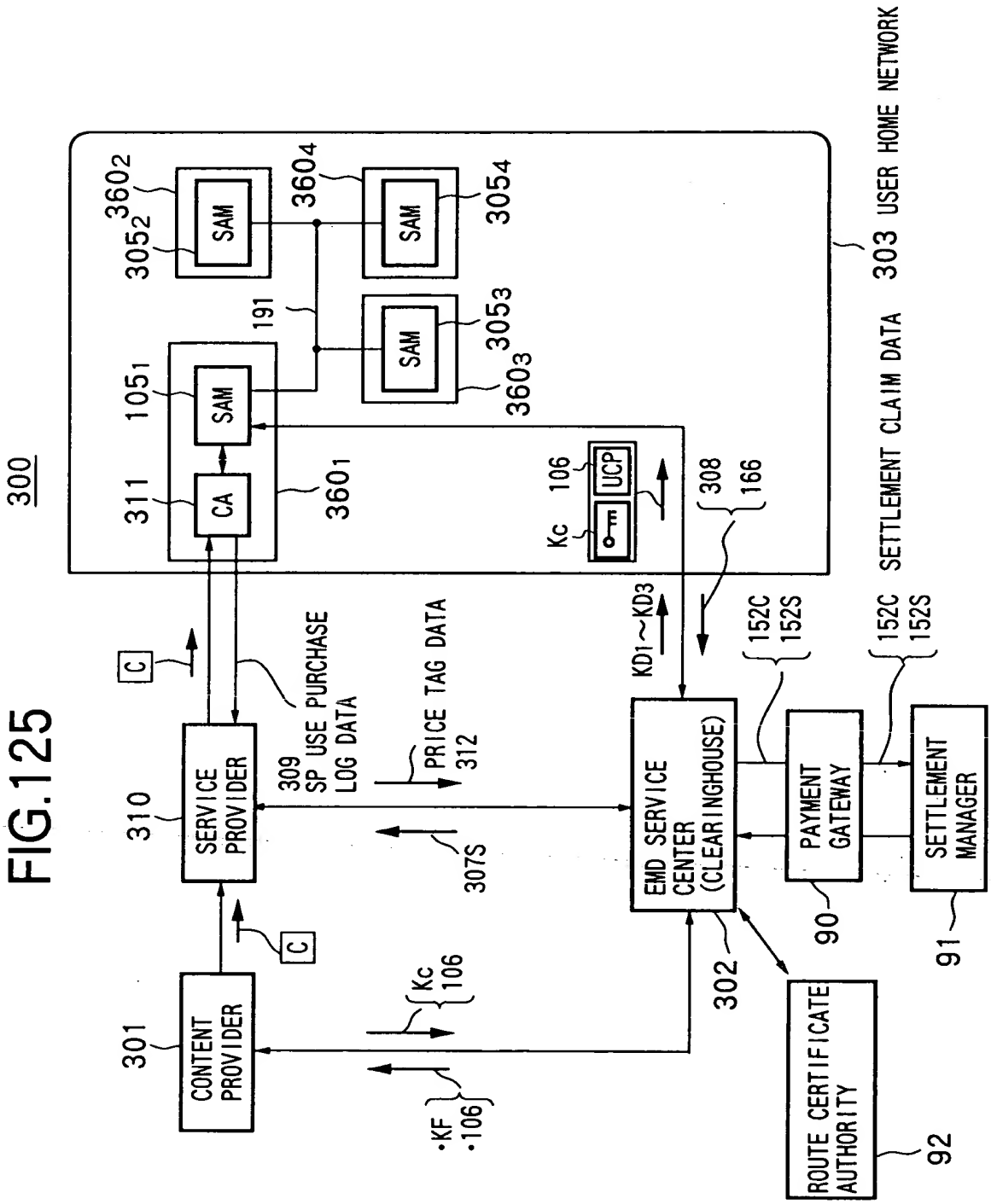

300
303 USER HOME NETWORK
SETTLEMENT CLAIM DATA
SAM
CA
UCP
Kc
106
308
166
191
311
105₁
360₁
360₂
360₃
360₄
305₂
305₃
305₄
C
309
SP USE PURCHASE LOG DATA
PRICE TAG DATA
312
307S
KD1~KD3
152C
152S
SERVICE PROVIDER
310
CONTENT PROVIDER
301
EMD SERVICE CENTER (CLEARINGHOUSE)
302
PAYMENT GATEWAY
90
SETTLEMENT MANAGER
91
ROUTE CERTIFICATE AUTHORITY
92
KF
106

FIG.126

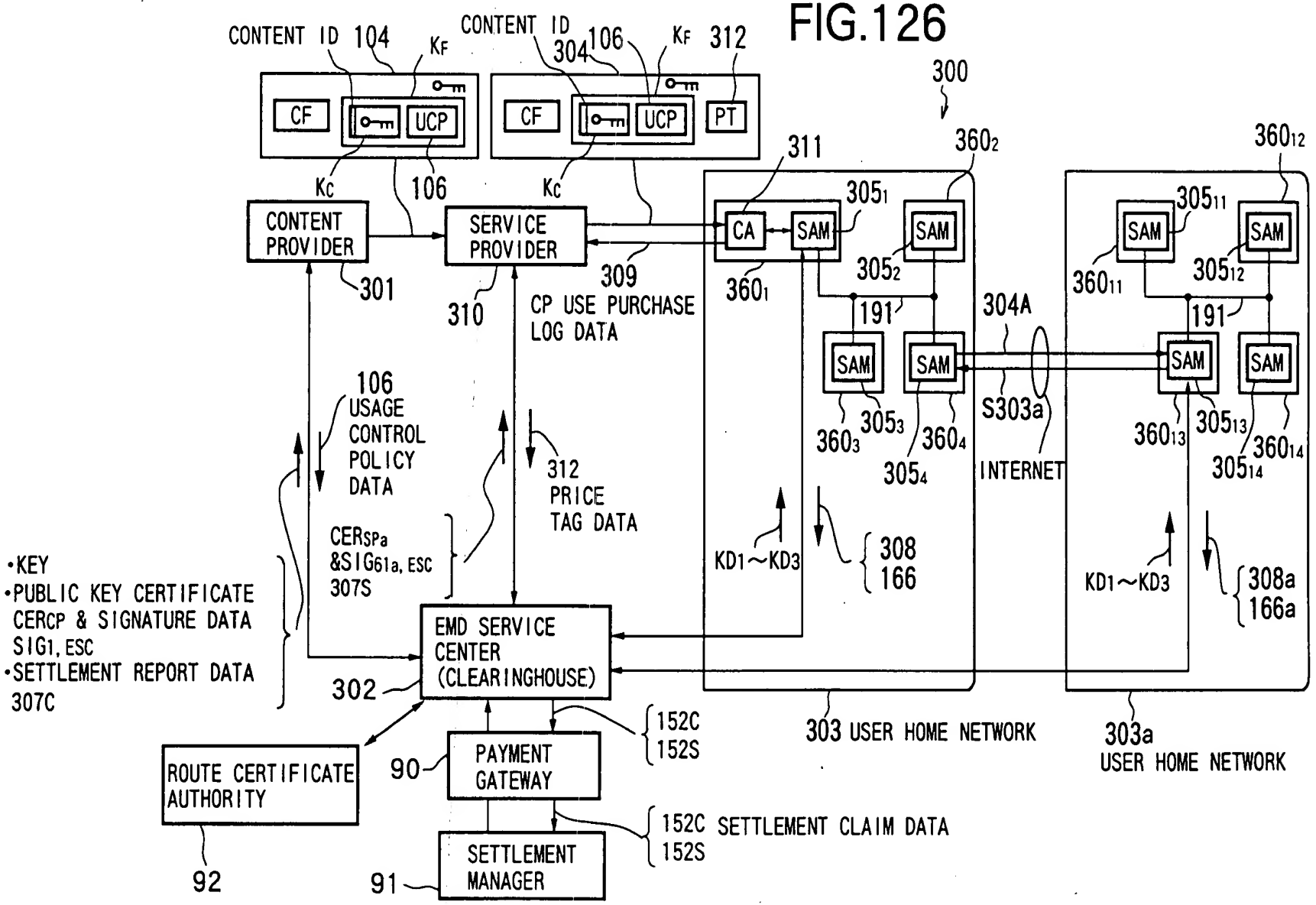

CONTENT ID 104
KF
CONTENT ID 304
106
KF 312
CF
UCP
CF
UCP
PT
300
311
360₂
360₁₂
Kc
106
Kc
CONTENT PROVIDER
SERVICE PROVIDER
CA
SAM
305₁
SAM
SAM
SAM
SAM
SAM
SAM
305₁₁
305₁₂
301
310
309
CP USE PURCHASE LOG DATA
360₁
305₂
360₁₁
191
191
304A
106
USAGE CONTROL POLICY DATA
312
PRICE TAG DATA
S303a
INTERNET
360₃
305₃
360₄
305₄
360₁₃
305₁₃
360₁₄
305₁₄
CERSPa &SIG61a, ESC 307S
KD1~KD3
308
166
KD1~KD3
308a
166a
•KEY
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 307C
EMD SERVICE CENTER (CLEARINGHOUSE)
302
152C
152S
303 USER HOME NETWORK
303a
USER HOME NETWORK
ROUTE CERTIFICATE AUTHORITY
90
PAYMENT GATEWAY
152C
152S
SETTLEMENT CLAIM DATA
92
91
SETTLEMENT MANAGER

FIG.127

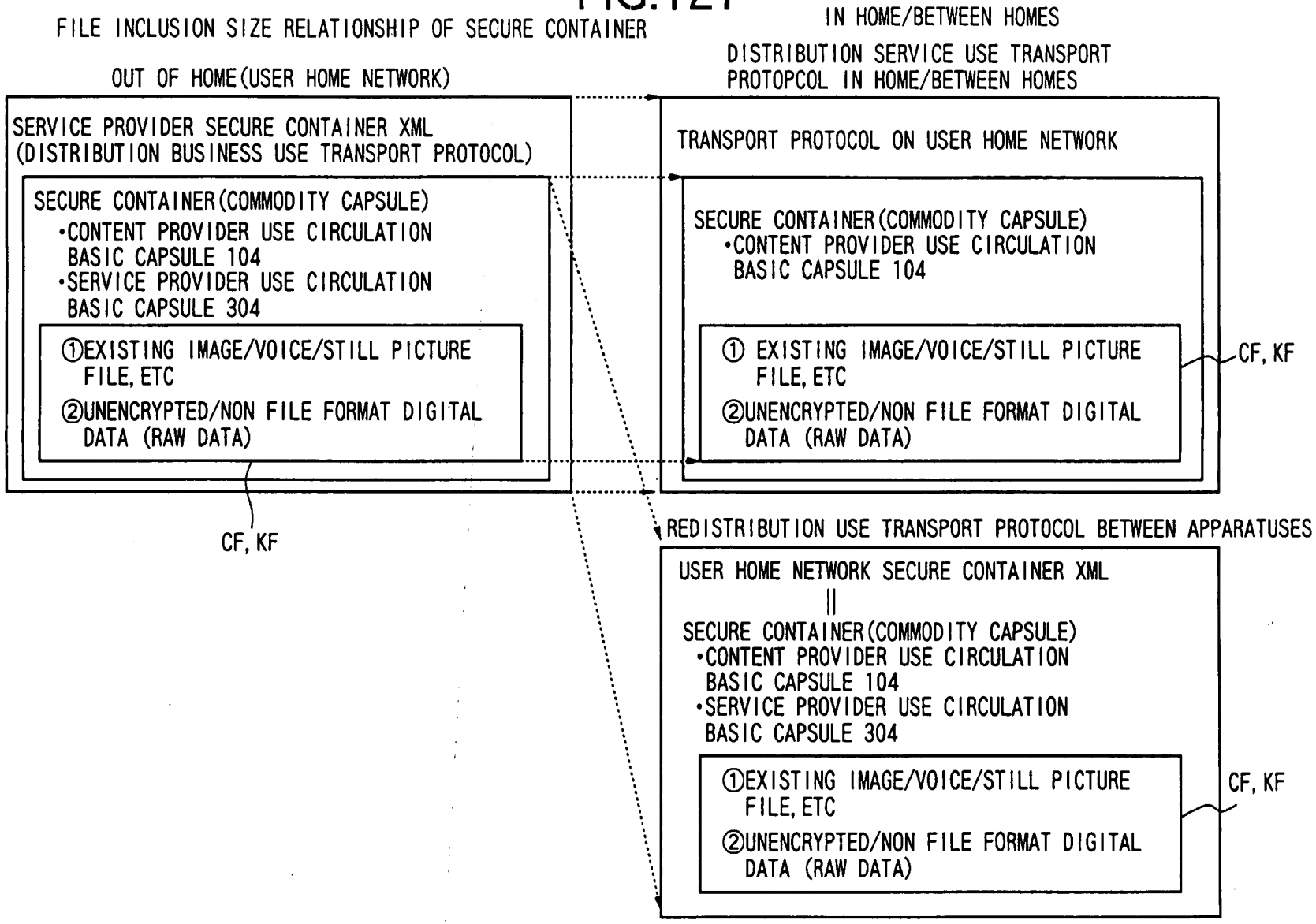

FILE INCLUSION SIZE RELATIONSHIP OF SECURE CONTAINER
OUT OF HOME(USER HOME NETWORK)
IN HOME/BETWEEN HOMES
DISTRIBUTION SERVICE USE TRANSPORT PROTOPCOL IN HOME/BETWEEN HOMES
SERVICE PROVIDER SECURE CONTAINER XML (DISTRIBUTION BUSINESS USE TRANSPORT PROTOCOL)
SECURE CONTAINER(COMMODITY CAPSULE)
•CONTENT PROVIDER USE CIRCULATION BASIC CAPSULE 104
•SERVICE PROVIDER USE CIRCULATION BASIC CAPSULE 304
①EXISTING IMAGE/VOICE/STILL PICTURE FILE, ETC
②UNENCRYPTED/NON FILE FORMAT DIGITAL DATA (RAW DATA)
CF, KF
TRANSPORT PROTOCOL ON USER HOME NETWORK
SECURE CONTAINER(COMMODITY CAPSULE)
•CONTENT PROVIDER USE CIRCULATION BASIC CAPSULE 104
① EXISTING IMAGE/VOICE/STILL PICTURE FILE, ETC
②UNENCRYPTED/NON FILE FORMAT DIGITAL DATA (RAW DATA)
CF, KF
REDISTRIBUTION USE TRANSPORT PROTOCOL BETWEEN APPARATUSES
USER HOME NETWORK SECURE CONTAINER XML
=
SECURE CONTAINER(COMMODITY CAPSULE)
•CONTENT PROVIDER USE CIRCULATION BASIC CAPSULE 104
•SERVICE PROVIDER USE CIRCULATION BASIC CAPSULE 304
①EXISTING IMAGE/VOICE/STILL PICTURE FILE, ETC
②UNENCRYPTED/NON FILE FORMAT DIGITAL DATA (RAW DATA)
CF, KF

FIG.128

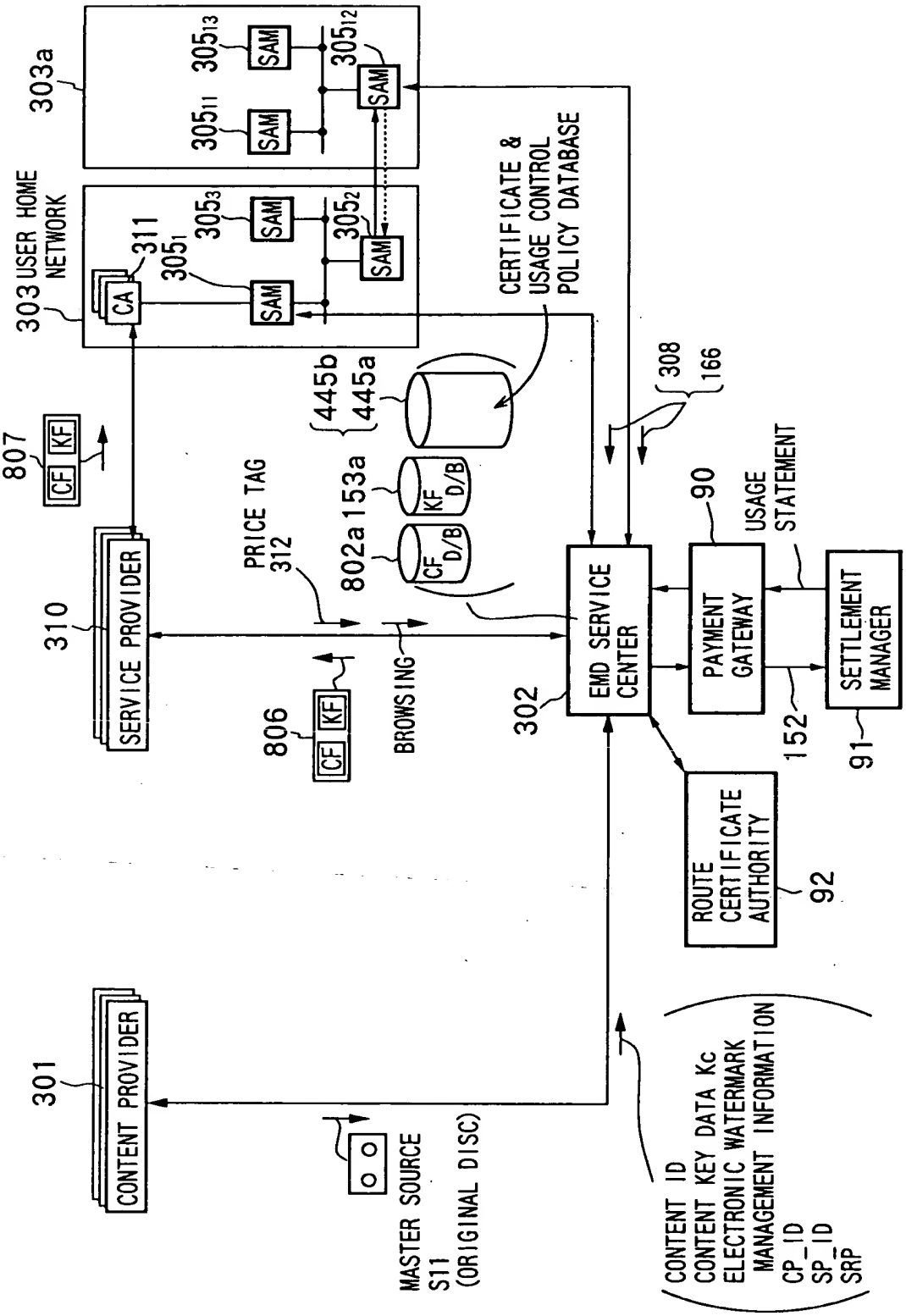

CONTENT PROVIDER
301
MASTER SOURCE
S11
(ORIGINAL DISC)
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP
SERVICE PROVIDER
310
807
CF
KF
806
CF
KF
PRICE TAG
312
BROWSING
802a
153a
CF D/B
KF D/B
445b
445a
CERTIFICATE &
USAGE CONTROL
POLICY DATABASE
303 USER HOME
NETWORK
CA
311
305₁
305₂
305₃
305₁₁
305₁₂
305₁₃
SAM
303a
308
166
EMD SERVICE
CENTER
302
PAYMENT
GATEWAY
90
USAGE
STATEMENT
SETTLEMENT
MANAGER
91
152
ROUTE
CERTIFICATE
AUTHORITY
92

FIG.129

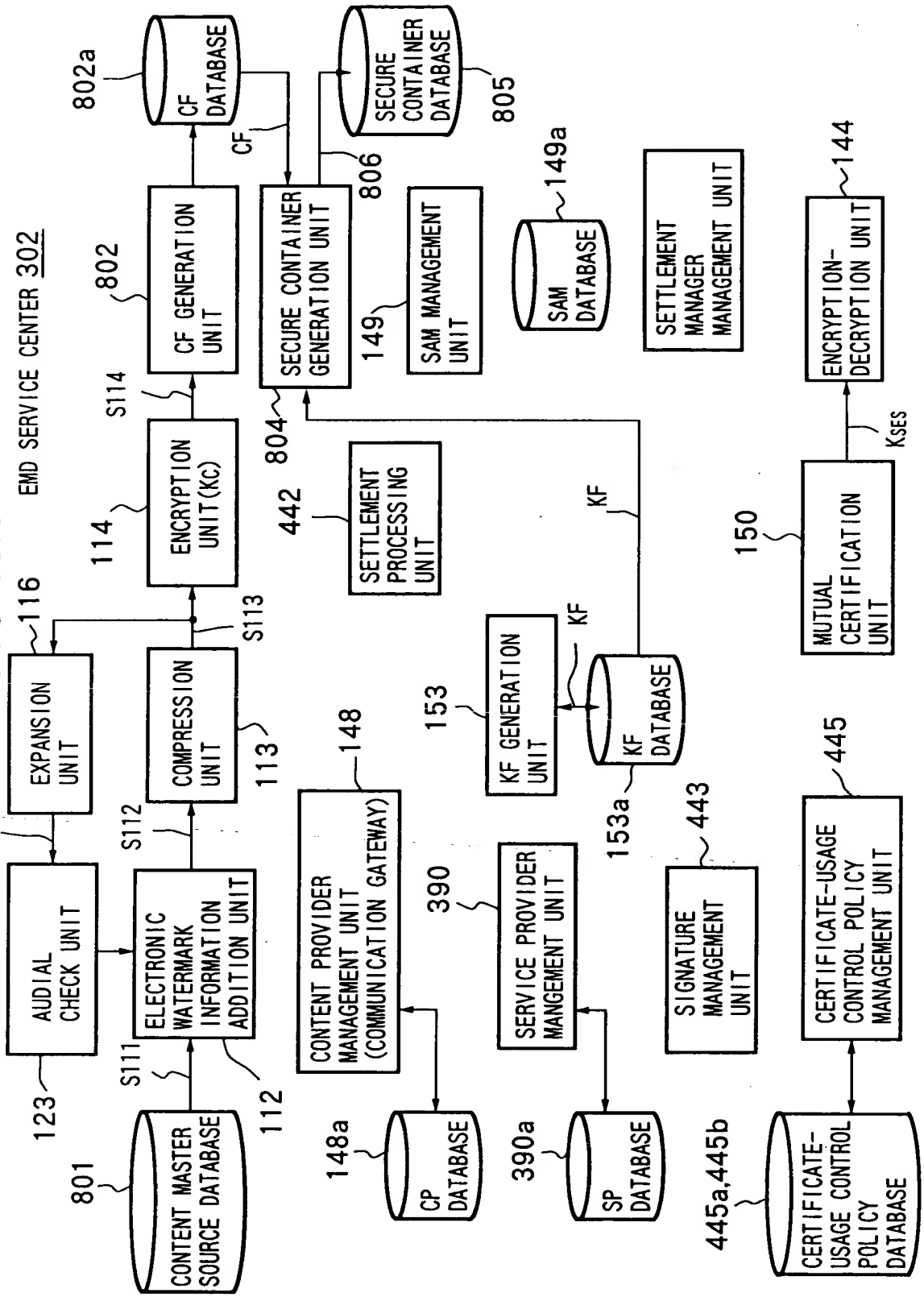

EMD SERVICE CENTER 302
CONTENT MASTER SOURCE DATABASE
801
AUDIAL CHECK UNIT
123
EXPANSION UNIT
116
ELECTRONIC WATERMARK INFORMATION ADDITION UNIT
112
COMPRESSION UNIT
113
ENCRYPTION UNIT(Kc)
114
CF GENERATION UNIT
802
CF DATABASE
802a
CF
SECURE CONTAINER GENERATION UNIT
804
SECURE CONTAINER DATABASE
805
806
SAM MANAGEMENT UNIT
149
SAM DATABASE
149a
SETTLEMENT MANAGER MANAGEMENT UNIT
SETTLEMENT PROCESSING UNIT
442
ENCRYPTION-DECRYPTION UNIT
144
MUTUAL CERTIFICATION UNIT
150
KSES
KF
KF GENERATION UNIT
153
KF DATABASE
153a
CONTENT PROVIDER MANAGEMENT UNIT (COMMUNICATION GATEWAY)
148
CP DATABASE
148a
SERVICE PROVIDER MANGEMENT UNIT
390
SP DATABASE
390a
SIGNATURE MANAGEMENT UNIT
443
CERTIFICATE-USAGE CONTROL POLICY MANAGEMENT UNIT
445
CERTIFICATE-USAGE CONTROL POLICY DATABASE
445a,445b
S111
S112
S113
S114
S116

FIG.130

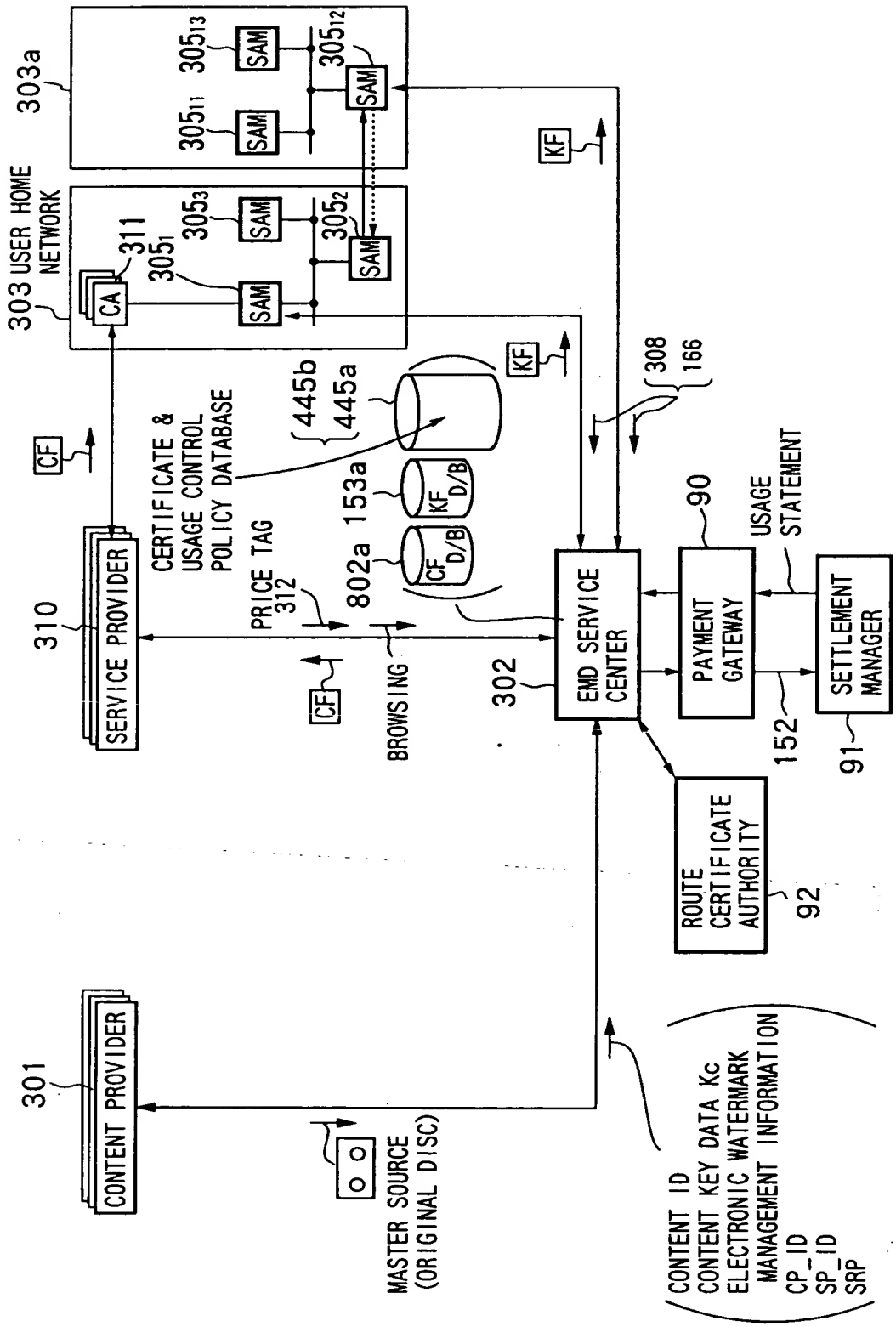

303a
303 USER HOME NETWORK
CA
311
SAM
KF
CF
445b
445a
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
153a
KF D/B
CF D/B
802a
310
SERVICE PROVIDER
PRICE TAG
312
BROWSING
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
USAGE STATEMENT
SETTLEMENT MANAGER
152
91
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
MASTER SOURCE (ORIGINAL DISC)
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.131

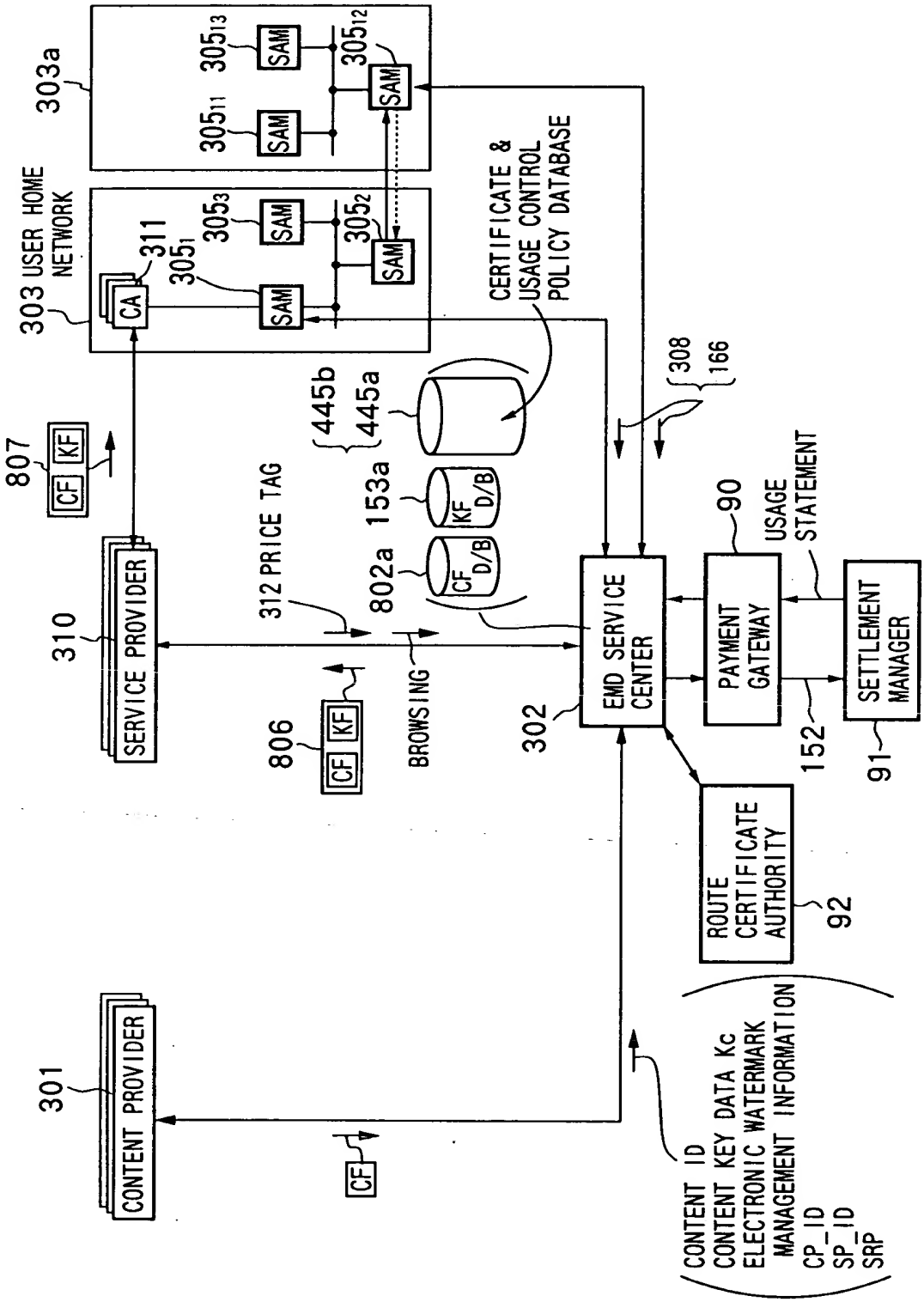

303a
305_{13}
305_{12}
305_{11}
SAM
303 USER HOME NETWORK
311
CA
305_1
305_3
305_2
CERTIFICATE & USAGE CONTROL POLICY DATABASE
445b
445a
308
166
807
CF
KF
153a
KF D/B
802a
CF D/B
312 PRICE TAG
310
SERVICE PROVIDER
806
BROWSING
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
USAGE STATEMENT
SETTLEMENT MANAGER
152
91
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.132

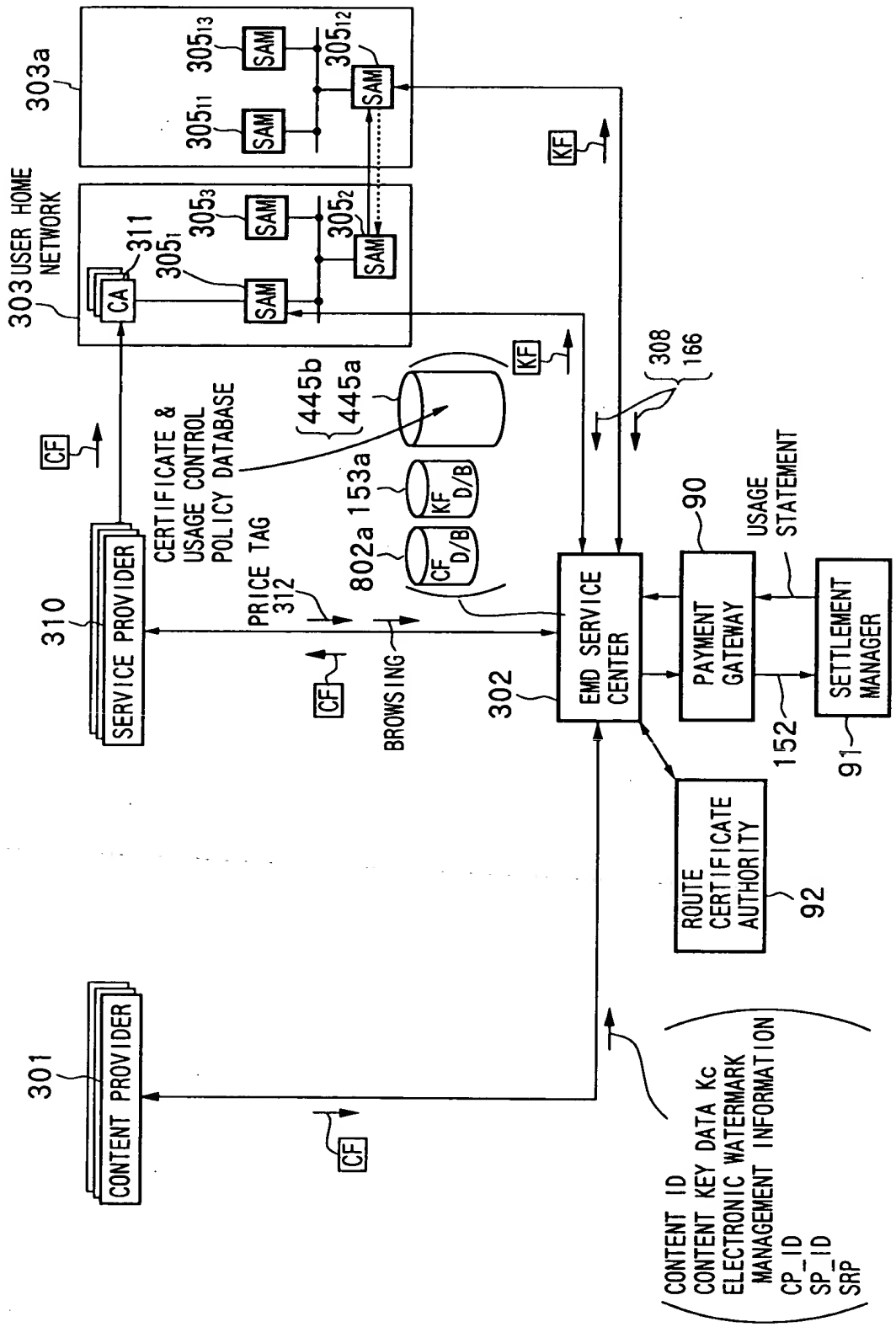

303a
305₁₃
305₁₂
305₁₁
SAM
303 USER HOME NETWORK
311
305₁
305₃
305₂
CA
KF
CF
445b
445a
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
153a
KF D/B
802a
CF D/B
310
SERVICE PROVIDER
PRICE TAG
312
BROWSING
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
USAGE STATEMENT
SETTLEMENT MANAGER
152
91
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.133

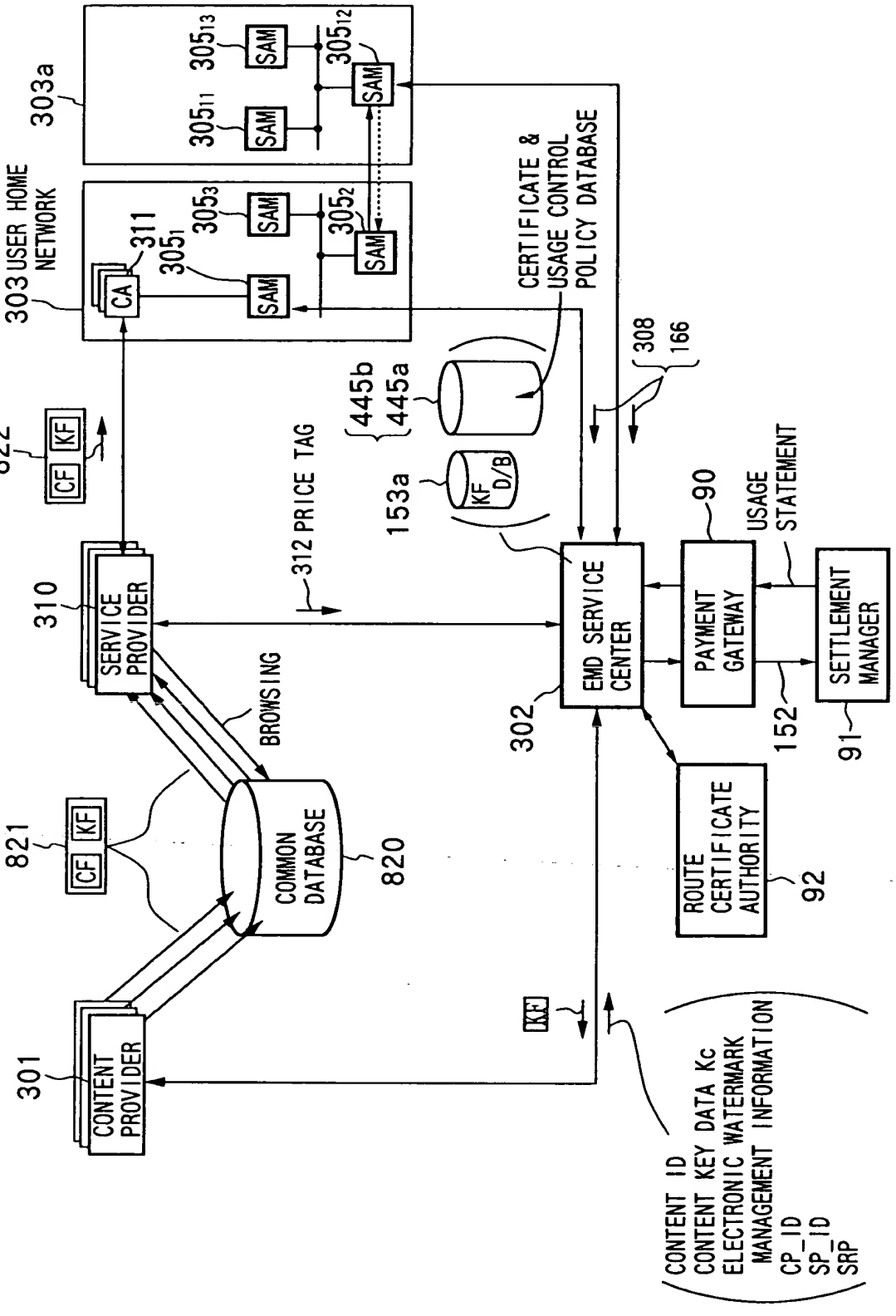

303a
305₁₃
305₁₂
305₁₁
SAM
303 USER HOME NETWORK
311
305₁
305₃
305₂
CA
SAM
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
445b
445a
822
CF
KF
312 PRICE TAG
153a
KF D/B
310
SERVICE PROVIDER
BROWSING
EMD SERVICE CENTER
302
90
PAYMENT GATEWAY
USAGE STATEMENT
SETTLEMENT MANAGER
152
91
821
COMMON DATABASE
820
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
KF
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.134

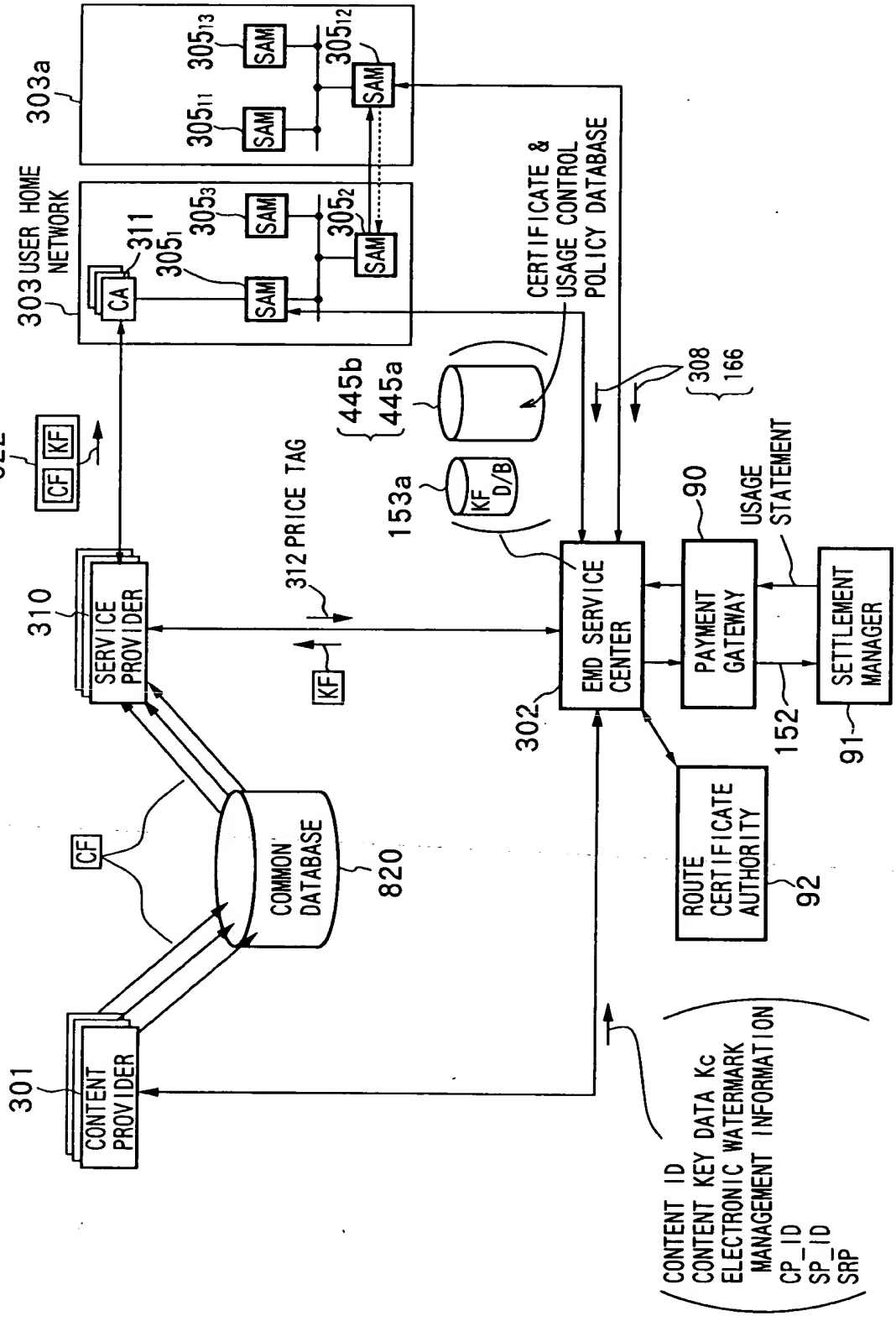

CONTENT PROVIDER
301
SERVICE PROVIDER
310
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP
CF
COMMON DATABASE
820
822
CF
KF
KF
312 PRICE TAG
EMD SERVICE CENTER
302
153a
KF D/B
445b
445a
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
PAYMENT GATEWAY
152
90
USAGE STATEMENT
SETTLEMENT MANAGER
91
ROUTE CERTIFICATE AUTHORITY
92
303 USER HOME NETWORK
CA
311
SAM
303a

FIG.135

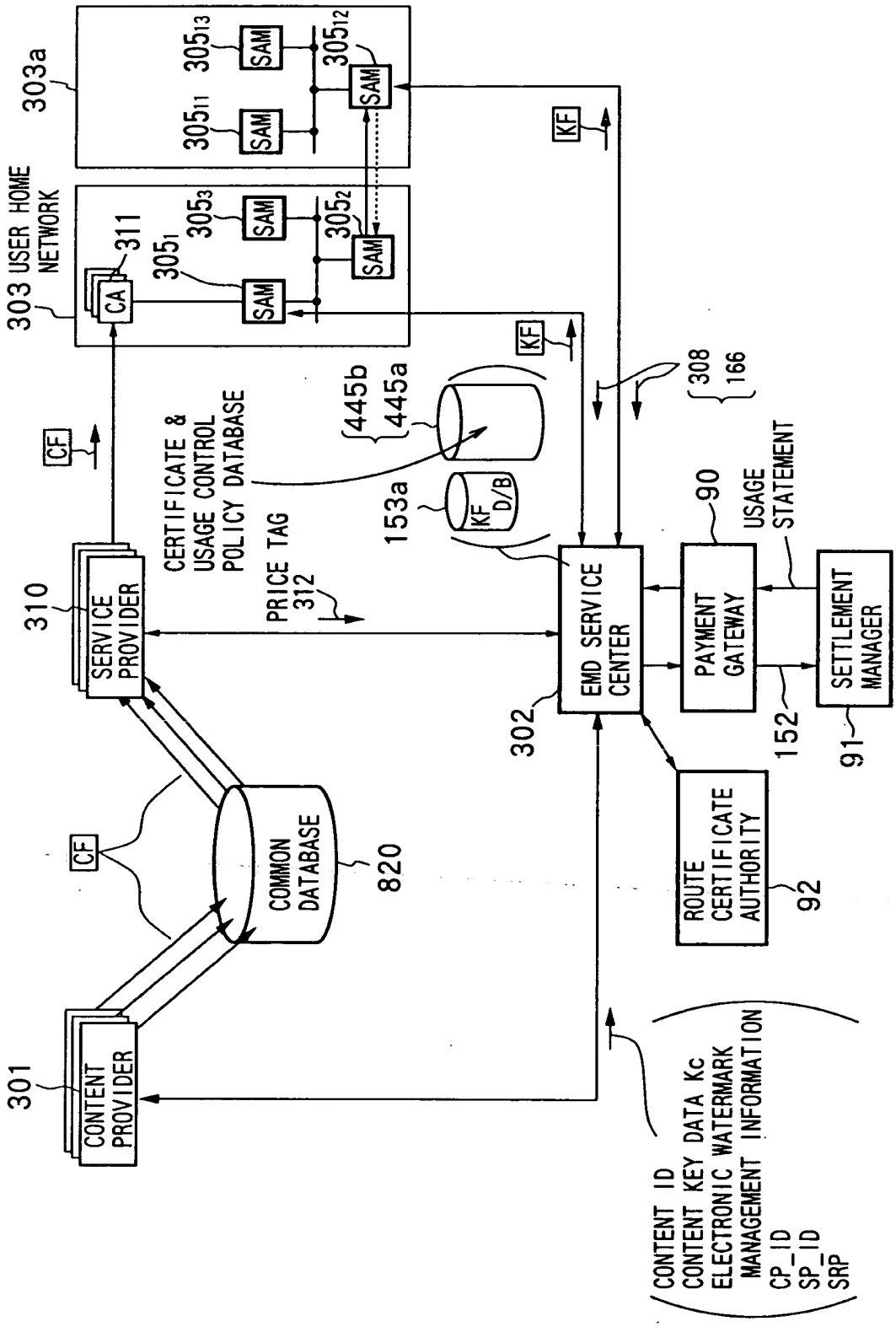

303a
305₁₃
305₁₂
305₁₁
SAM
303 USER HOME NETWORK
311
CA
305₁
305₃
305₂
KF
CF
445b
445a
308
166
CERTIFICATE & USAGE CONTROL POLICY DATABASE
153a
KF D/B
90
USAGE STATEMENT
310
SERVICE PROVIDER
PRICE TAG 312
EMD SERVICE CENTER
PAYMENT GATEWAY
SETTLEMENT MANAGER
302
152
91
COMMON DATABASE
820
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.136

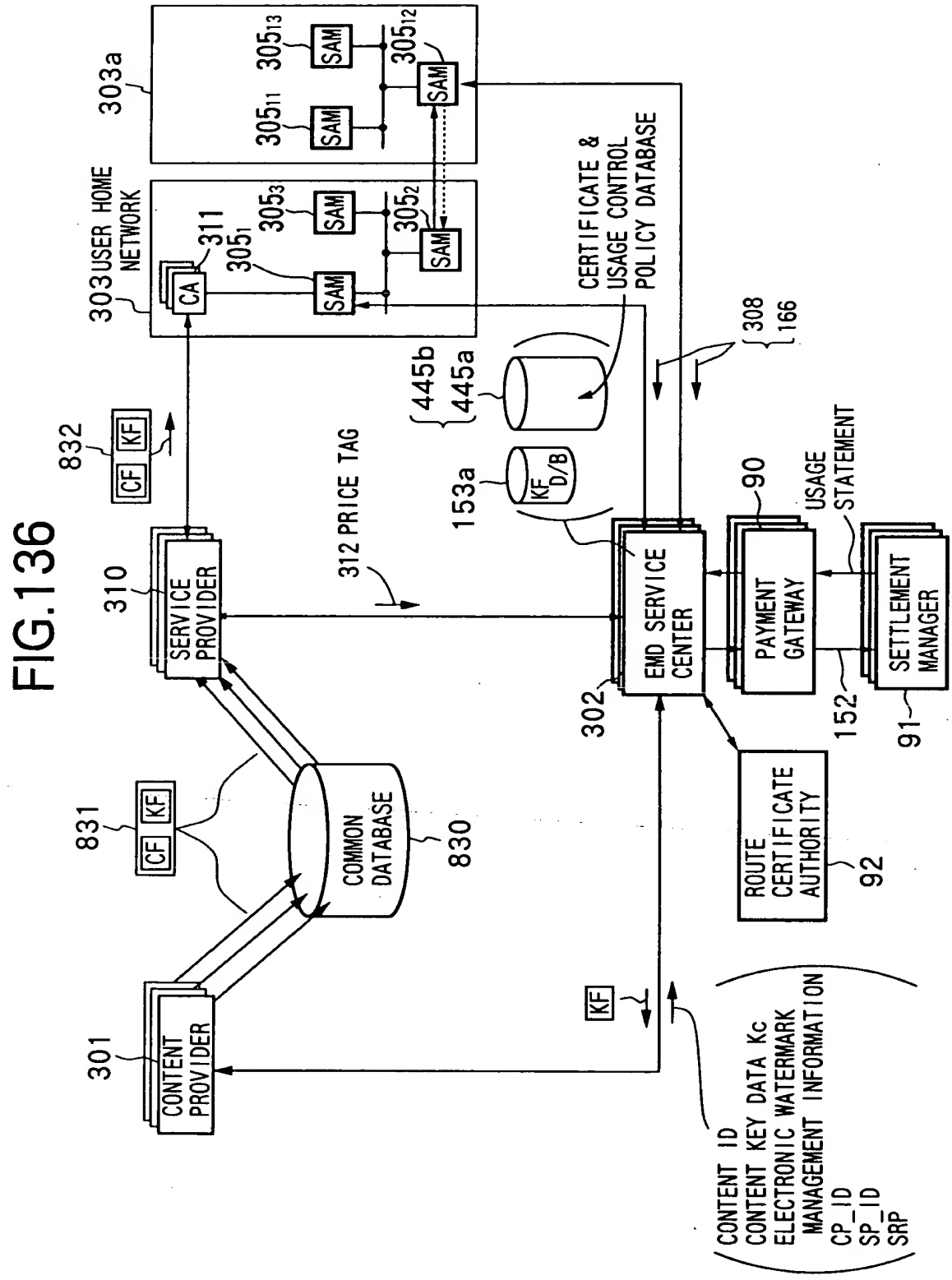

303a
303 USER HOME NETWORK
305_{13}
305_{12}
305_{11}
305_3
305_2
305_1
311
SAM
CA
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
445b
445a
832
CF
KF
153a
$KF_{D/B}$
312 PRICE TAG
310
SERVICE PROVIDER
EMD SERVICE CENTER
302
90
PAYMENT GATEWAY
USAGE STATEMENT
SETTLEMENT MANAGER
152
91
831
COMMON DATABASE
830
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.137

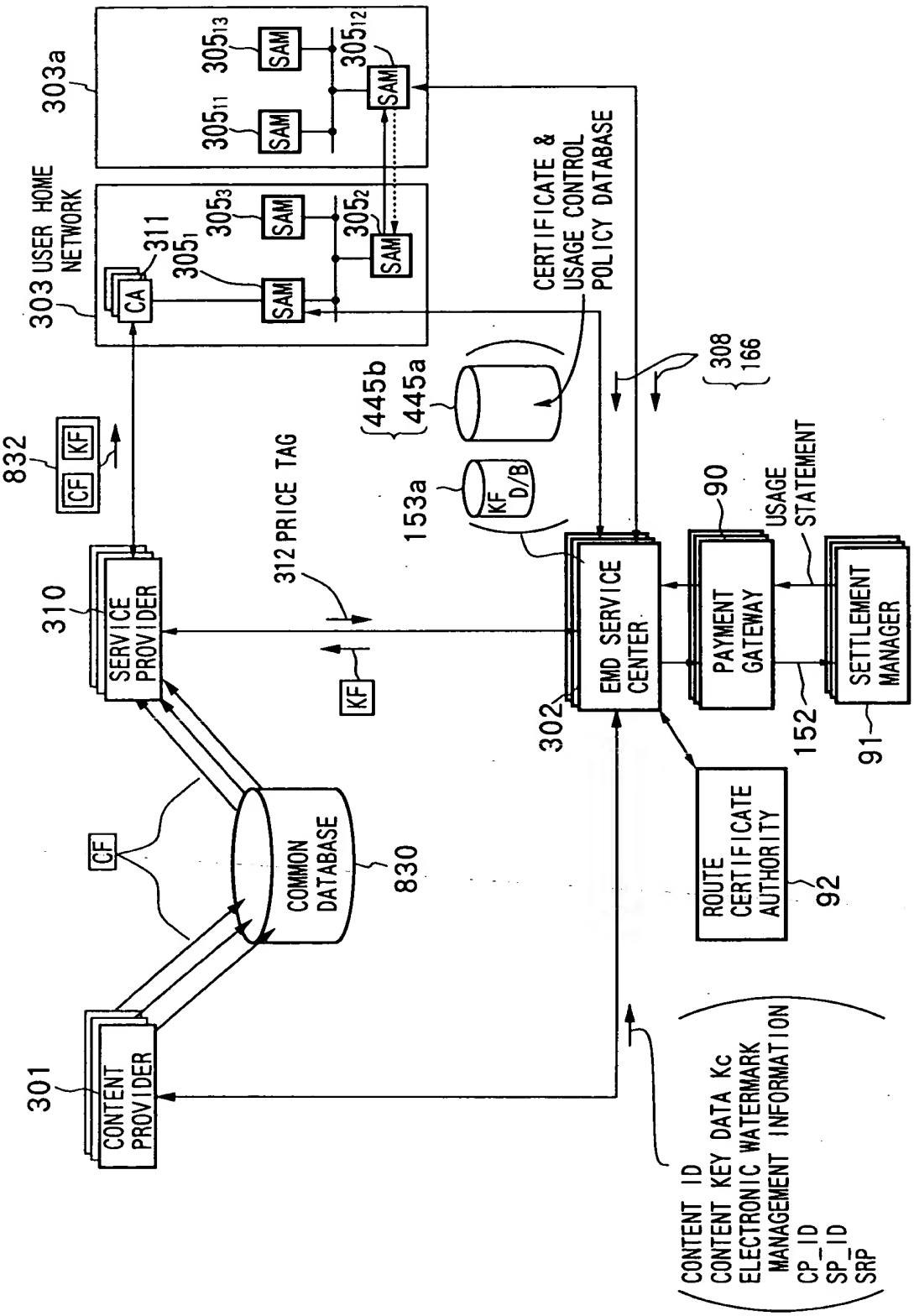

303a
305₁₃
SAM
305₁₂
SAM
305₁₁
SAM
303 USER HOME NETWORK
311
CA
305₁
SAM
305₃
SAM
305₂
SAM
CERTIFICATE & USAGE CONTROL POLICY DATABASE
445b
445a
308
166
832
CF
KF
312 PRICE TAG
153a
KF D/B
90
USAGE STATEMENT
310
SERVICE PROVIDER
KF
302
EMD SERVICE CENTER
PAYMENT GATEWAY
SETTLEMENT MANAGER
152
91
CF
COMMON DATABASE
830
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.138

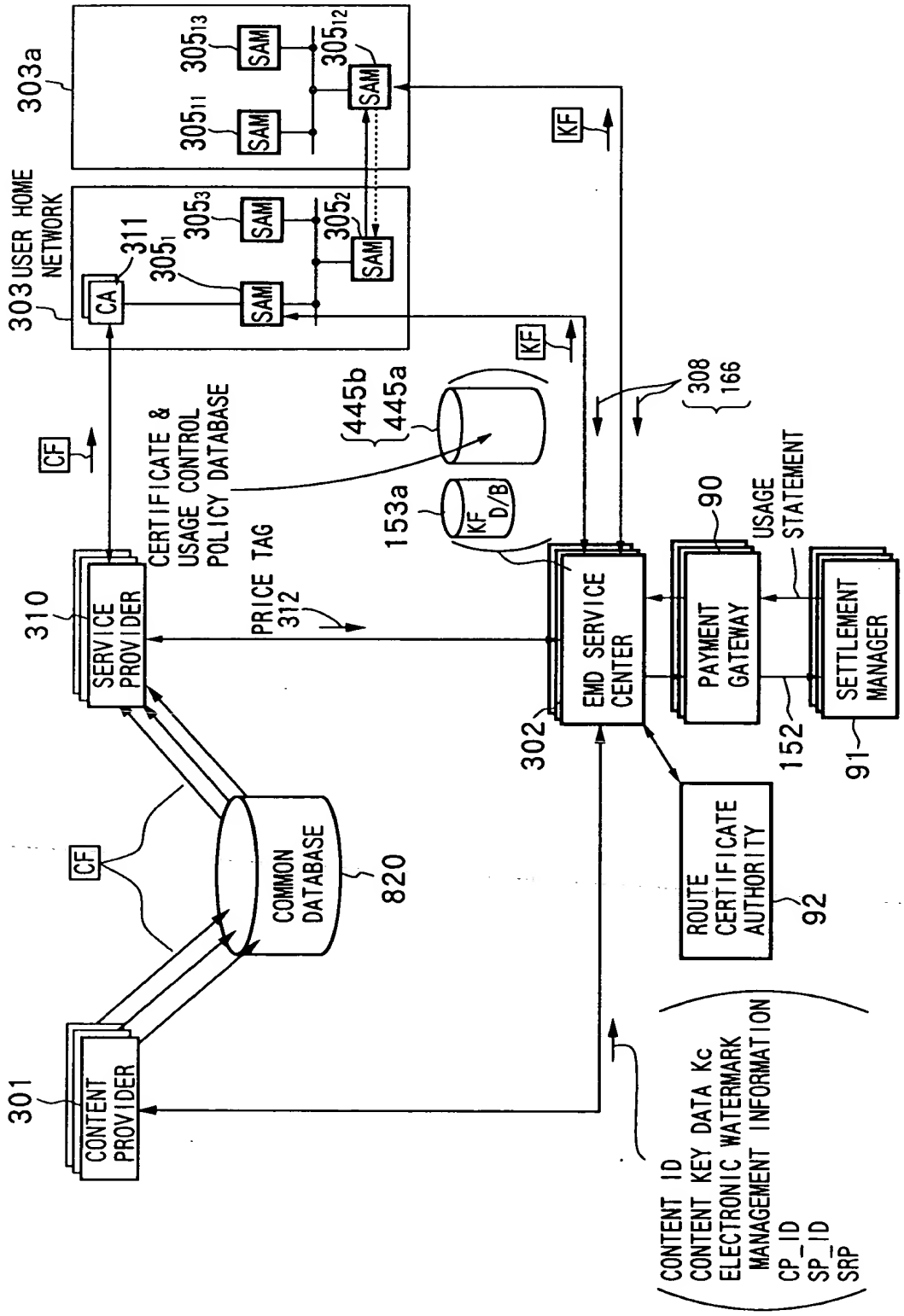

303a
SAM
305_{13}
305_{12}
305_{11}
303 USER HOME NETWORK
CA
311
305_1
305_3
305_2
KF
445b
445a
308
166
CF
CERTIFICATE & USAGE CONTROL POLICY DATABASE
153a
KF D/B
90
USAGE STATEMENT
310
SERVICE PROVIDER
PRICE TAG
312
EMD SERVICE CENTER
PAYMENT GATEWAY
SETTLEMENT MANAGER
302
152
91
COMMON DATABASE
820
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.139

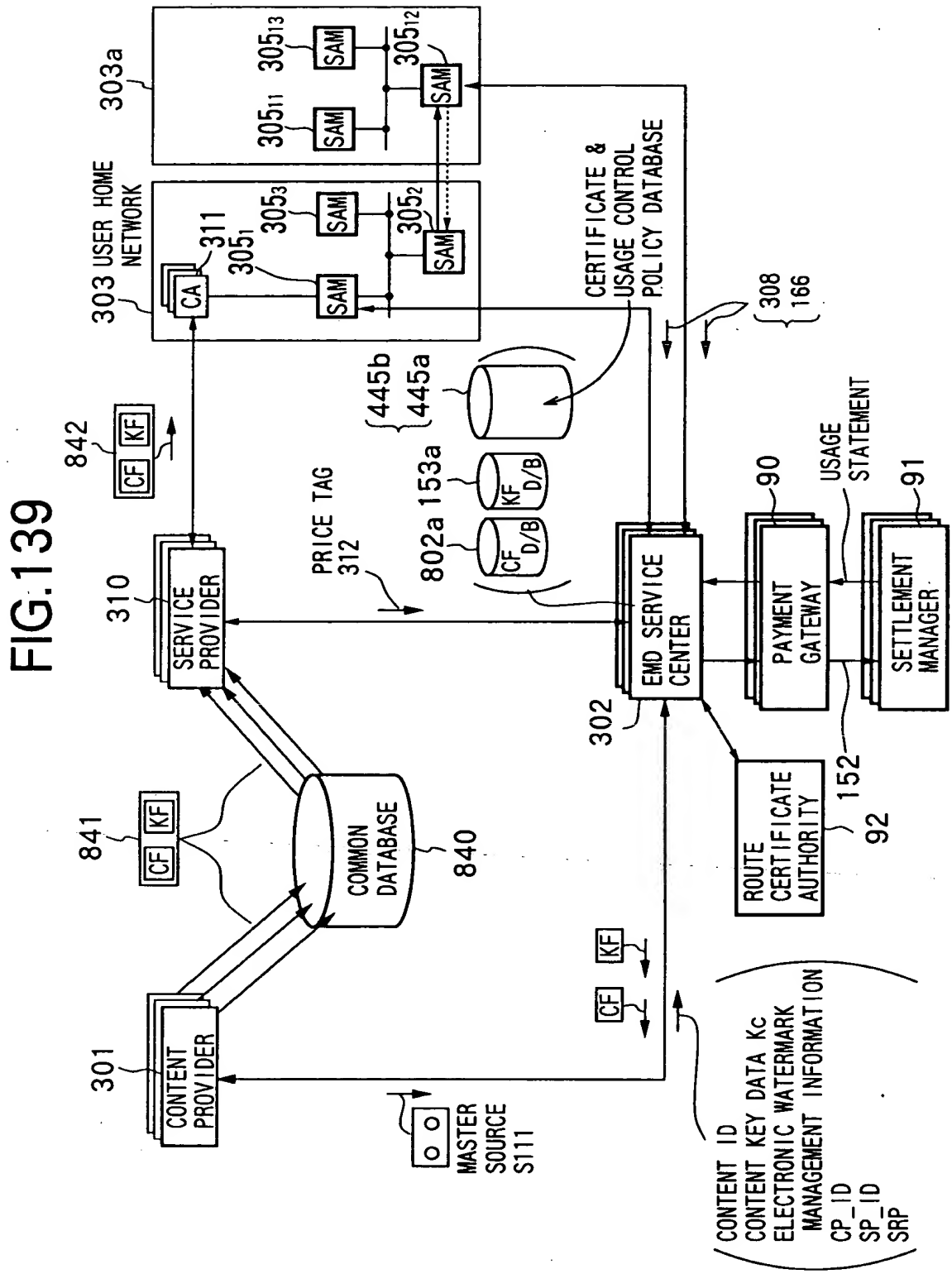

303a
303 USER HOME NETWORK
305_{13}
305_{12}
305_{11}
305_3
305_2
305_1
311
SAM
CA
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
445b
445a
842
CF
KF
153a
KF D/B
802a
CF D/B
PRICE TAG
312
310
SERVICE PROVIDER
EMD SERVICE CENTER
302
90
PAYMENT GATEWAY
USAGE STATEMENT
91
SETTLEMENT MANAGER
841
COMMON DATABASE
840
ROUTE CERTIFICATE AUTHORITY
152
92
301
CONTENT PROVIDER
MASTER SOURCE
S111
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.140

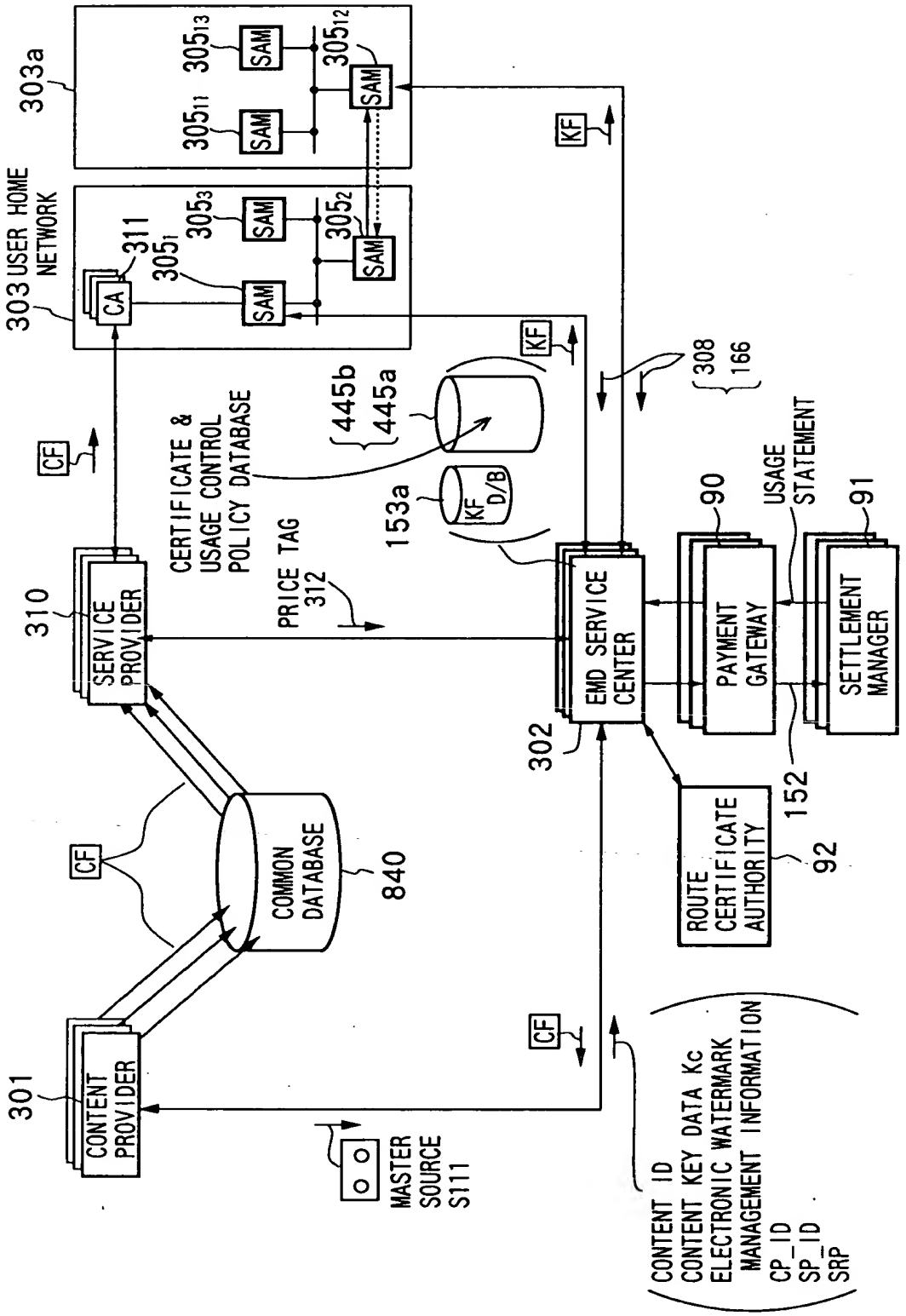

303a
303 USER HOME NETWORK
305_{13}
305_{12}
305_{11}
305_3
305_2
305_1
SAM
311
CA
KF
CF
445b
445a
CERTIFICATE & USAGE CONTROL POLICY DATABASE
308
166
153a
KF D/B
PRICE TAG
312
310
SERVICE PROVIDER
90
USAGE STATEMENT
91
EMD SERVICE CENTER
PAYMENT GATEWAY
SETTLEMENT MANAGER
302
152
COMMON DATABASE
840
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER
MASTER SOURCE S111
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.141

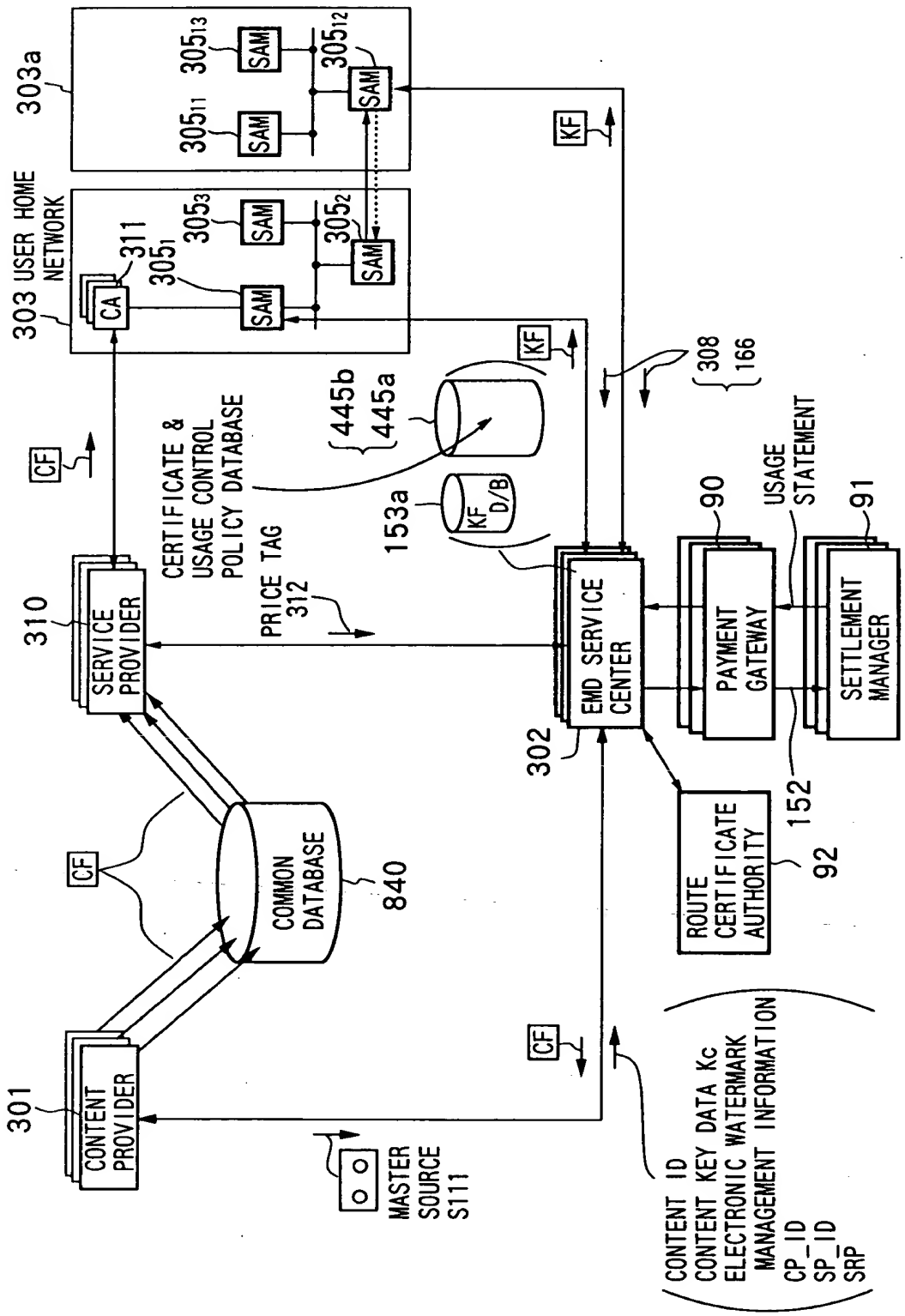

303a
305₁₃
305₁₂
305₁₁
SAM
303 USER HOME NETWORK
CA
311
305₁
305₃
305₂
KF
CF
445b
445a
308
166
CERTIFICATE & USAGE CONTROL POLICY DATABASE
153a
KF D/B
310
SERVICE PROVIDER
PRICE TAG
312
EMD SERVICE CENTER
302
90
PAYMENT GATEWAY
USAGE STATEMENT
91
SETTLEMENT MANAGER
152
ROUTE CERTIFICATE AUTHORITY
92
COMMON DATABASE
840
301
CONTENT PROVIDER
MASTER SOURCE S111
CONTENT ID
CONTENT KEY DATA Kc
ELECTRONIC WATERMARK
MANAGEMENT INFORMATION
CP_ID
SP_ID
SRP

FIG.142

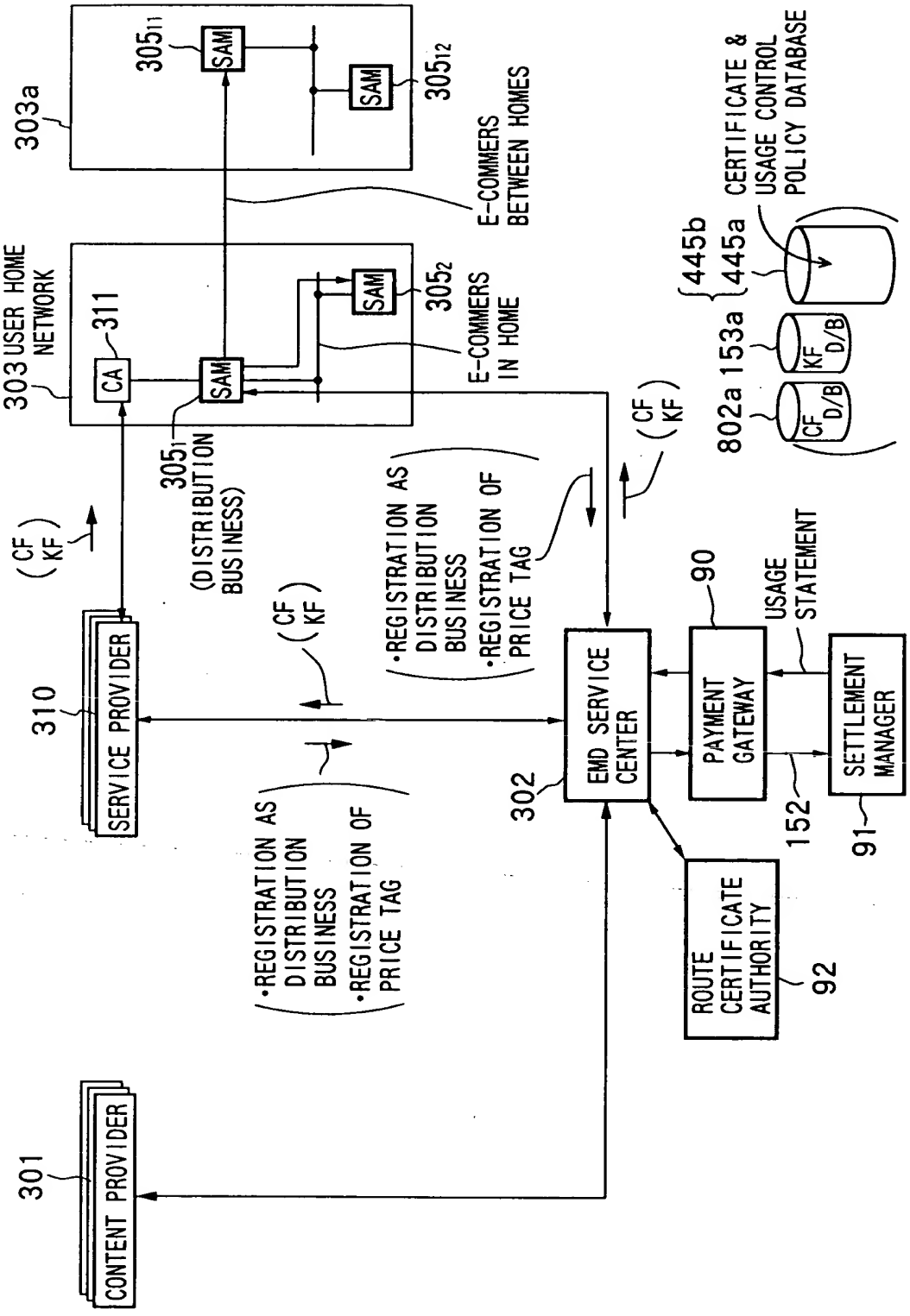

303a
305₁₁
SAM
305₁₂
SAM
E-COMMERS BETWEEN HOMES
303 USER HOME NETWORK
CA
311
SAM
305₂
SAM
E-COMMERS IN HOME
305₁ (DISTRIBUTION BUSINESS)
445b
445a
CERTIFICATE & USAGE CONTROL POLICY DATABASE
802a
CF D/B
153a
KF D/B
(CF KF)
(CF KF)
(CF KF)
•REGISTRATION AS DISTRIBUTION BUSINESS
•REGISTRATION OF PRICE TAG
•REGISTRATION AS DISTRIBUTION BUSINESS
•REGISTRATION OF PRICE TAG
310
SERVICE PROVIDER
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
USAGE STATEMENT
152
91
SETTLEMENT MANAGER
ROUTE CERTIFICATE AUTHORITY
92
301
CONTENT PROVIDER

FIG.143

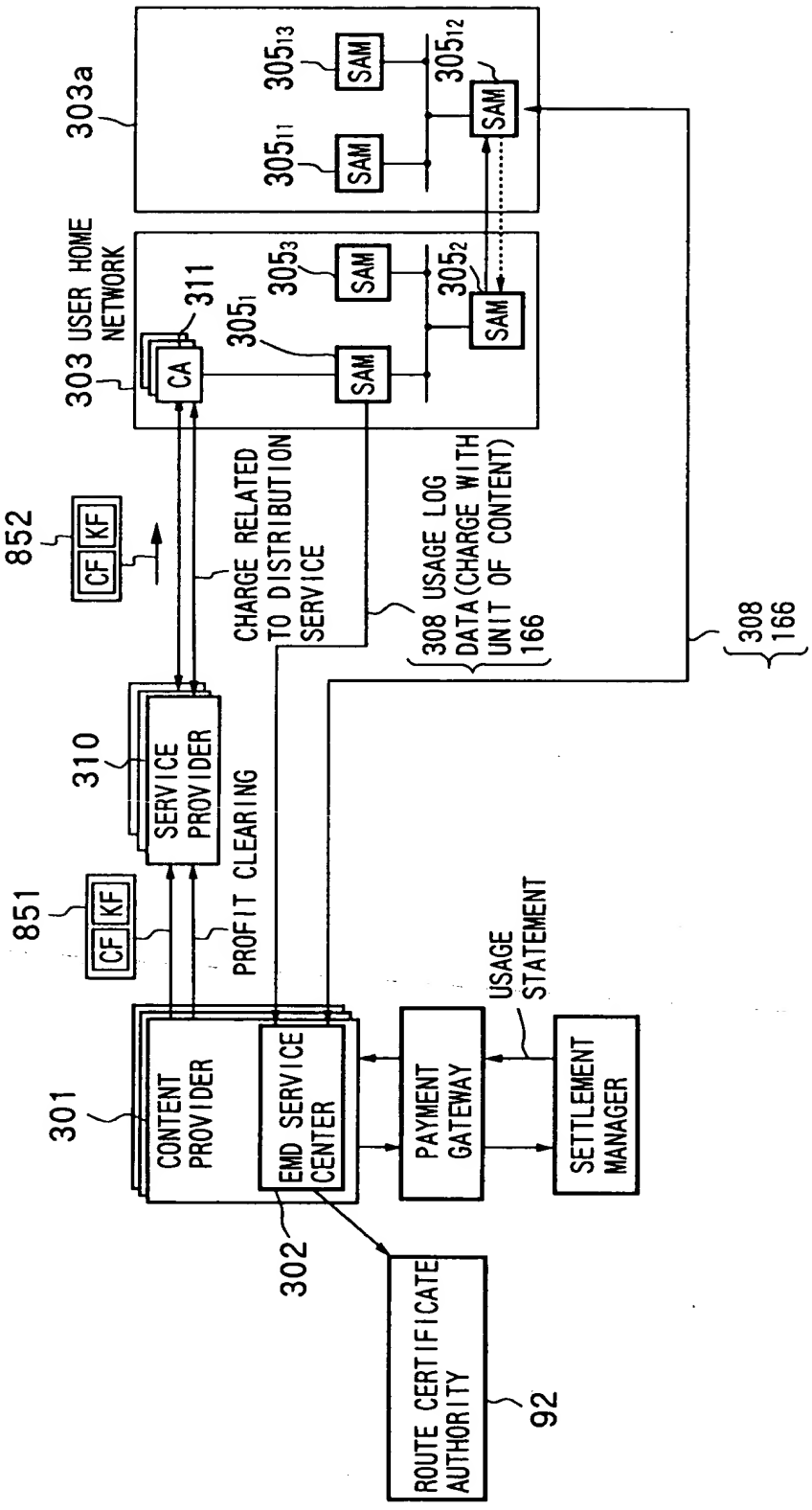

303a
305₁₃
305₁₂
305₁₁
SAM
303 USER HOME NETWORK
311
CA
305₃
305₂
305₁
852
CF
KF
CHARGE RELATED TO DISTRIBUTION SERVICE
308 USAGE LOG DATA(CHARGE WITH UNIT OF CONTENT)
166
308
166
310
SERVICE PROVIDER
851
PROFIT CLEARING
USAGE STATEMENT
301
CONTENT PROVIDER
EMD SERVICE CENTER
PAYMENT GATEWAY
SETTLEMENT MANAGER
302
ROUTE CERTIFICATE AUTHORITY
92

FIG.144

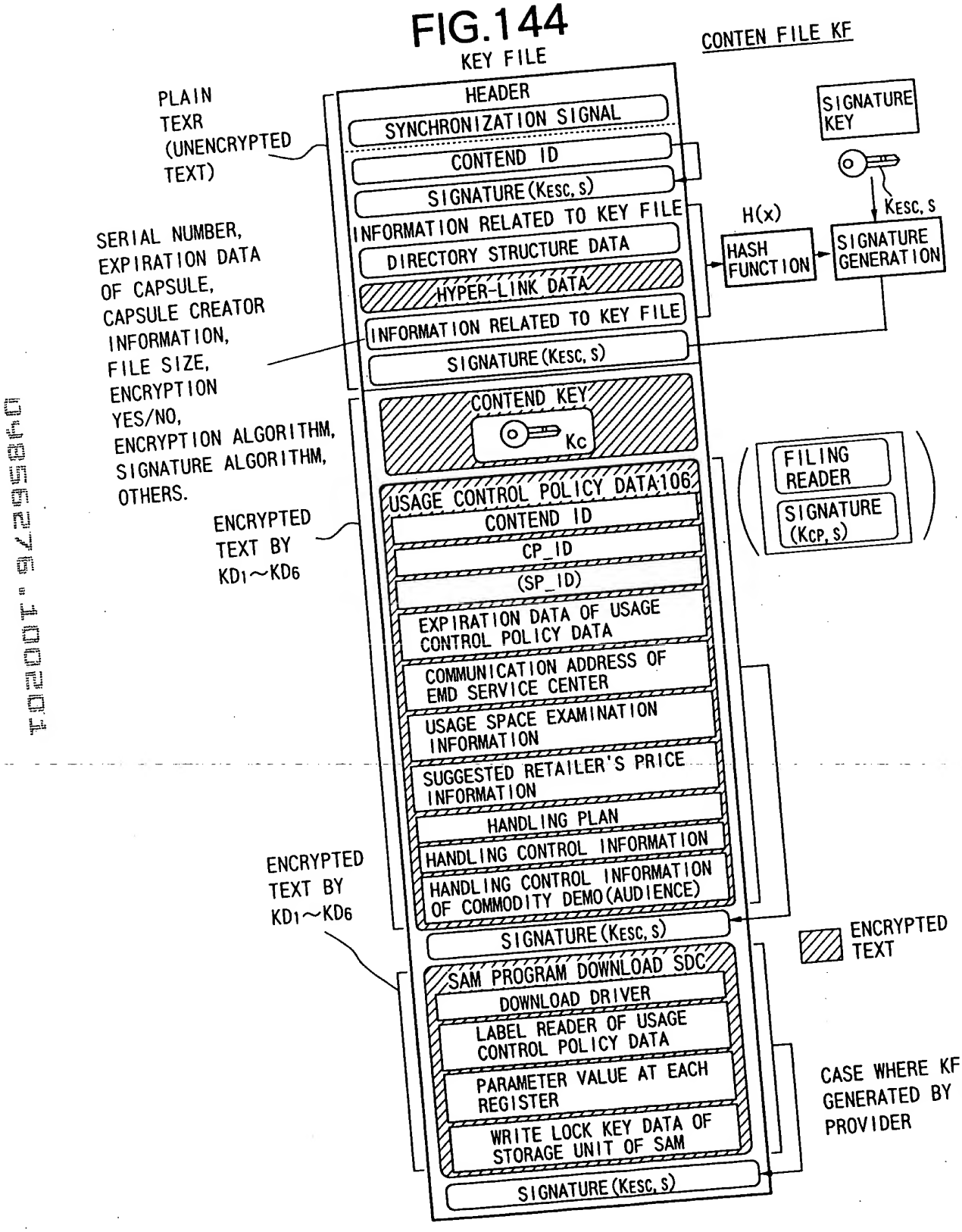
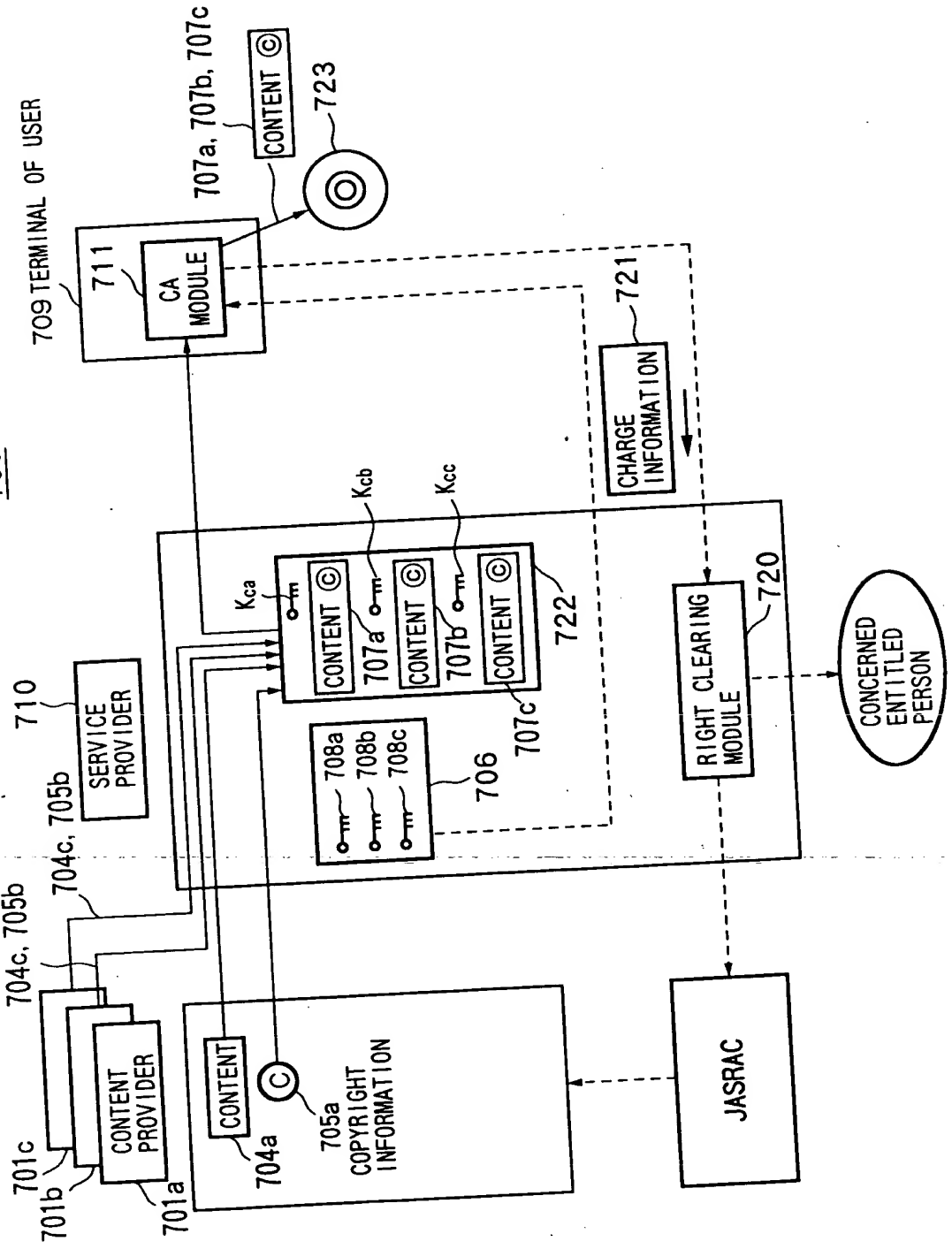


FIG.145


700
709 TERMINAL OF USER
711
CA MODULE
707a, 707b, 707c
CONTENT ©
723
721
CHARGE INFORMATION
Kca
Kcb
Kcc
CONTENT ©
707a
707b
707c
722
710
SERVICE PROVIDER
705b
704c, 705b
704c
708a
708b
708c
706
RIGHT CLEARING MODULE
720
CONCERNED ENTITLED PERSON
701c
701b
CONTENT PROVIDER
701a
CONTENT
704a
©
705a
COPYRIGHT INFORMATION
JASRAC

LIST OF REFERENCE NUMERALS

90... payment gateway

91... settlement manager

92... route certificate authority

100, 300... EMD system

101, 301... content provider

102, 302... EMD service center

103, 303... user home network

104, 304... secure container

105_1 to 105_4, 305_1 to 305_4... SAM

106... usage control policy data

107, 307... settlement report data

108, 308... usage log data

160_1... network apparatus

160_2 to 160_4... AV apparatuses

152, 152c, 152s... settlement claim data

191... bus

310... service provider

311... CA module

312... price tag data

CF... content file

KF... key file

Kc... content key data